# A unified approach to computing real and complex zeros of zero-dimensional ideals

Lasserre, J.B.; Laurent, M.; Rostalski, P.

*Published in:*
Emerging Applications of Algebraic Geometry

*Publication date:*
2009

# A UNIFIED APPROACH TO COMPUTING REAL AND COMPLEX ZEROS OF ZERO-DIMENSIONAL IDEALS

JEAN BERNARD LASSERRE*, MONIQUE LAURENT†, AND PHILIPP ROSTALSKI‡

**Abstract.** In this paper we propose a unified methodology for computing the set $V_{\mathbb{K}}(I)$ of complex ($\mathbb{K} = \mathbb{C}$) or real ($\mathbb{K} = \mathbb{R}$) roots of an ideal $I \subseteq \mathbb{R}[x]$, assuming $V_{\mathbb{K}}(I)$ is finite. We show how moment matrices, defined in terms of a given set of generators of the ideal $I$, can be used to (numerically) find not only the real variety $V_{\mathbb{R}}(I)$, as shown in the authors' previous work, but also the complex variety $V_{\mathbb{C}}(I)$, thus leading to a unified treatment of the algebraic and real algebraic problem. In contrast to the real algebraic version of the algorithm, the complex analogue only uses basic numerical linear algebra because it does not require positive semidefiniteness of the moment matrix and so avoids semidefinite programming techniques. The links between these algorithms and other numerical algebraic methods are outlined and their stopping criteria are related.

**Key words.** Polynomial ideal, zero-dimensional ideal, complex roots, real roots, numerical linear algebra.

**AMS(MOS) subject classifications.** 12D10, 12E12, 12Y05, 13A15.

## 1. Introduction.

**1.1. Motivation and contribution.** Computing all complex and/or real solutions of a system of polynomial equations is a fundamental problem in mathematics with many important practical applications. Let $I \subseteq \mathbb{R}[x] := \mathbb{R}[x_1, \ldots, x_n]$ be an ideal generated by a set of polynomials $h_j$ $(j = 1, \ldots, m)$. Fundamental problems in polynomial algebra are:

**(I)** The computation of the algebraic variety $V_{\mathbb{C}}(I) = \{v \in \mathbb{C}^n \mid h_j(v) = 0 \; \forall \; j = 1, \ldots, m\}$ of $I$,

**(II)** The computation of the real variety $V_{\mathbb{R}}(I) = V_{\mathbb{C}}(I) \cap \mathbb{R}^n$ of $I$,

as well as a set of generators for the radical ideal $J = I(V_{\mathbb{K}}(I))$ for $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$, assuming $V_{\mathbb{K}}(I)$ is finite.

One way to solve problem (II) is to first compute all complex solutions and to sort out $V_{\mathbb{R}}(I) = \mathbb{R}^n \cap V_{\mathbb{C}}(I)$ from $V_{\mathbb{C}}(I)$ afterwards. This is certainly possible when $I$ is a zero-dimensional ideal, but even in this case one might perform many unnecessary computations, particularly if $|V_{\mathbb{R}}(I)| \ll |V_{\mathbb{C}}(I)|$, i.e. in case there are many more complex than real roots. In addition there are cases where $V_{\mathbb{R}}(I)$ is finite whereas $V_{\mathbb{C}}(I)$ is not! These two reasons

*LAAS-CNRS and Institute of Mathematics, Toulouse, France (lasserre@laas.fr). Supported by the french national research agency ANR under grant NT05-3-41612.

†Centrum voor Wiskunde en Informatica, Kruislaan 413, 1098 SJ Amsterdam, Netherlands (M.Laurent@cwi.nl). Supported by the Netherlands Organization for Scientific Research grant NWO 639.032.203 and by ADONET, Marie Curie Research Training Network MRTN-CT-2003-504438.

‡Automatic Control Laboratory, Physikstrasse 3, ETH Zurich, 8092 Zurich, Switzerland (rostalski@control.ee.ethz.ch).

alone provide a rationale for designing a method specialized to problem (II), that is, a method that takes into account right from the beginning the *real* algebraic nature of the problem.

In [10] we have provided a semidefinite characterization and an algorithm for approximating $V_{\mathbb{K}}(I)$ ($\mathbb{K} = \mathbb{R}, \mathbb{C}$) as well as a basis of the radical ideal $I(V_{\mathbb{K}}(I))$ (in the form of a border or Gröbner basis). The approach there utilizes well established semidefinite programming techniques and numerical linear algebra. Remarkably, all information needed to compute the above objects is contained in the so-called moment matrix (a matrix with a particular quasi-Hankel structure, indexed by a basis of $\mathbb{R}[x]$, and whose entries depend on the polynomials generating the ideal $I$) and the geometry behind it when this matrix is required to be positive semidefinite with maximum rank. For the task of computing the real roots and the real radical ideal $\sqrt[\mathbb{R}]{I} = I(V_{\mathbb{R}}(I))$, the method is real algebraic in nature, as we do not compute (implicitly or explicitly) any complex element of $V_{\mathbb{C}}(I)$.

The method proposed in [10] for solving problem (I) treats $\mathbb{C}^n$ as $\mathbb{R}^{2n}$ and essentially applies the same algorithm as for problem (II), but now working in $\mathbb{R}^{2n}$ instead of $\mathbb{R}^n$. Hence one has to use semidefinite matrices of much larger size since they are now indexed by a basis of $\mathbb{C}[x, \bar{x}]$ (as opposed to $\mathbb{R}[x]$ for problem (II)).

This latter remark is one of the motivations for the present paper in which we provide a method for computing $V_{\mathbb{C}}(I)$, a complex analogue of the method of [10] for computing $V_{\mathbb{R}}(I)$, which also uses a moment matrix indexed by a basis of $\mathbb{R}[x]$ (instead of $\mathbb{C}[x, \overline{x}]$ as in [10]). The algorithm is very similar to the one proposed in [10] for problem (II), except for the important fact that we now do *not* require the positivity of the moment matrix; therefore the algorithm only uses basic numerical linear algebra techniques and *no* semidefinite programming optimization. The price to pay for the reduced complexity is that our algorithm now finds a basis for an ideal $J$ with $I \subseteq J \subseteq \sqrt{I}$ (instead of $J = \sqrt{I}$ in [10]), though with the same algebraic variety $V_{\mathbb{C}}(J) = V_{\mathbb{C}}(I)$. Note however that once a basis $\mathcal{B}$ of $\mathbb{R}[x]/J$ and the corresponding multiplication matrices are known, generators for the ideal $\sqrt{I}$ can be computed numerically e.g. via the algorithm proposed in [7].

On the other hand there is a plethora of methods and algorithms to compute the (finite) complex variety $V_{\mathbb{C}}(I)$ and certain distinguished bases as Gröbner and border bases to name just a few. This motivates the second contribution of this paper, which is to relate the proposed method based on moment matrices to existing methods and, in particular, to the method of [18] (and [17]) for the (finite) complex variety. It turns out that, by adding the positive semidefiniteness constraint, the method of [18] can be adapted and extended for computing the (finite) real variety $V_{\mathbb{R}}(I)$; this will be treated in detail in the follow-up paper [9]. Summarizing, our results provide a unified treatment of the computation of real and complex

roots either by means of moment matrices or by means of a dual form characterization as in [9], [17] and [18].

**1.2. Related literature.** The importance and relevance to various branches of mathematics of the problem of solving systems of polynomials is reflected by the broad literature, see e.g. [6]. Various methods exist for problem (I), ranging from numerical continuation methods (see e.g. [22]), to exact symbolic methods (e.g. [19]), or more general symbolic/numeric methods (e.g. [16] or [18], see also the monograph [23]). For instance, Verschelde [24] proposes a numerical algorithm via homotopy continuation methods (cf. also [22]) whereas Rouillier [19] solves a zero-dimensional system of polynomials symbolically by giving a rational univariate representation (RUR) for its solutions, of the form $f(t) = 0$, $x_1 = \frac{g_1(t)}{g(t)}$, ..., $x_n = \frac{g_n(t)}{g(t)}$, where $f, g, g_1, \ldots, g_n \in \mathbb{K}[t]$ are univariate polynomials. The computation of the RUR relies in an essential way on the multiplication matrices in the quotient algebra $\mathbb{K}[x]/I$ which thus requires the knowledge of a corresponding linear basis of the quotient space.

The literature tailored to problem (II), i.e. to the real solving of systems of polynomials, is by far not as broad as the one for finding all (complex) solutions. Most algorithms (beside our previous work [10]) are based on real-root counting algorithms using e.g. Hermite's quadratic forms or variants of Sturm sequences (see e.g. [1] or [20] for a discussion).

**1.3. Contribution.** Our first contribution is a unified treatment of the cases $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$ to obtain the 0-dimensional variety $V_{\mathbb{K}}(I)$. We will work with the space $\mathbb{R}[x]_t$ of polynomials of degree smaller or equal to $t$ and with certain subsets of its dual space $(\mathbb{R}[x]_t)^*$, the space of linear functionals on $\mathbb{R}[x]_t$. More precisely, for an integer $t \geq D := \max_j \deg(h_j)$, set

$$\mathcal{H}_t := \{h_j x^\alpha \mid j = 1, \ldots, m \text{ and } \alpha \in \mathbb{N}^n \text{ with } |\alpha| + \deg(h_j) \leq t\} \quad (1.1)$$

and consider the two sets

$$\mathcal{K}_t := \left\{ L \in (\mathbb{R}[x]_t)^* \;\middle|\; L(p) = 0 \ \forall p \in \mathcal{H}_t \right\} \quad (1.2)$$

for computing $V_{\mathbb{C}}(I)$, and

$$\mathcal{K}_{t,\succeq} := \left\{ L \in \mathcal{K}_t \;\middle|\; L(f^2) \geq 0 \ \ \forall f \in \mathbb{R}[x]_{\lfloor t/2 \rfloor} \right\} \quad (1.3)$$

for computing $V_{\mathbb{R}}(I)$. Obviously, the linear form associated with evaluation at $v \in V_{\mathbb{K}}(I)$, lies in the set $\mathcal{K}_{t,\succeq}$ ($\mathbb{K} = \mathbb{R}$) and its real and imaginary parts lie in the set $\mathcal{K}_t$ ($\mathbb{K} = \mathbb{C}$). Roughly speaking, by iterating on $t \in \mathbb{N}$, we will refine the description of those sets by successively adding linear conditions (and conditions stemming from SOS relations in $I$ in the case $\mathbb{K} = \mathbb{R}$), until they contain sufficient information to enable extraction of the points $V_{\mathbb{K}}(I)$.

**Sketch of the moment-matrix algorithm.** Let us now give a more specific sketch of the algorithm of [10] for $V_{\mathbb{R}}(I)$ and of its extension for $V_{\mathbb{C}}(I)$ proposed in the present paper. Given $L \in (\mathbb{R}[x]_t)^*$ and $1 \leq s \leq \lfloor t/2 \rfloor$, define its moment matrix $M_s(L)$ as the matrix indexed by $\mathbb{N}^n_s = \{\alpha \in \mathbb{N}^n \mid |\alpha| = \sum_i \alpha_i \leq s\}$, with $(\alpha, \beta)$th entry $L(x^\alpha x^\beta)$. For a matrix $M$, positive semidefiniteness, i.e. the property $x^T M x \geq 0$ for all vectors $x$, is denoted by $M \succeq 0$. Thus $L$ satisfies the condition $L(f^2) \geq 0$ for all $f \in \mathbb{R}[x]_{\lfloor t/2 \rfloor}$, precisely when $M_{\lfloor t/2 \rfloor}(L) \succeq 0$. Consider the following rank conditions on the matrix $M_s(L)$:

$$\operatorname{rank} M_s(L) = \operatorname{rank} M_{s-1}(L), \tag{1.4}$$

$$\operatorname{rank} M_s(L) = \operatorname{rank} M_{s-d}(L), \tag{1.5}$$

after setting $d := \lceil D/2 \rceil$. Algorithm 1 is our moment-matrix algorithm for finding $V_{\mathbb{K}}(I)$.

**Algorithm 1** *The moment-matrix algorithm for $V_{\mathbb{K}}(I)$:*

**Input:** $t \geq D$.

**Output:** A basis $\mathcal{B} \subseteq \mathbb{R}[x]_{s-1}$ of $\mathbb{K}[x]/\langle \operatorname{Ker} M_s(L) \rangle$ (which will enable the computation of $V_{\mathbb{K}}(I)$).

1: Find a generic element $L \in K_t$.
2: Check if (1.4) holds for some $D \leq s \leq \lfloor t/2 \rfloor$, or if (1.5) holds for some $d \leq s \leq \lfloor t/2 \rfloor$.
3: **if** yes **then**
4: **return** a basis $\mathcal{B} \subseteq \mathbb{R}[x]_{s-1}$ of the column space of $M_{s-1}(L)$,
5: **else**
6: Iterate (go to 1)) replacing $t$ by $t+1$
7: **end if**

REMARK 1.1. Here $K_t = \mathcal{K}_{t,\succeq}$ for the task of computing $V_{\mathbb{R}}(I)$ as in [10], and $K_t = \mathcal{K}_t$ for the task of computing $V_{\mathbb{C}}(I)$ in the present paper. In Step 1, we say that $L \in K_t$ is generic if, for all $1 \leq s \leq \lfloor t/2 \rfloor$, $\operatorname{rank} M_s(L)$ is maximum over $K_t$.

Consider first the real case, treated in [10]. A first observation is that in the above definition of a generic element, it suffices to require the maximum rank property for $s = \lfloor t/2 \rfloor$. The algorithm relies on the following crucial properties. If the answer in Step 2 is 'yes' then $\langle \operatorname{Ker} M_s(L) \rangle$, the ideal generated by polynomials $p$ of degree no more than $s$ whose coefficient vector $\operatorname{vec}(p)$ lies in $\operatorname{Ker} M_s(L)$, coincides with $I(V_{\mathbb{R}}(I))$, the real radical of $I$. Moreover the set $\mathcal{B}$ is a basis of the quotient space $\mathbb{R}[x]/\langle \operatorname{Ker} M_s(L) \rangle$ and thus one can apply the classical eigenvalue method to compute $V_{\mathbb{R}}(I)$. Additionally, a border (or Gröbner) basis of $I(V_{\mathbb{R}}(I))$ is readily available from the kernel of the matrix $M_s(L)$ (cf. [10] for details).

We show in the present paper that the *same* algorithm works also for the task of computing finite $V_{\mathbb{C}}(I)$ (whenever finite), except we now use

the set $K_t = \mathcal{K}_t$. Although the algorithms are apparently identical in the real and complex cases, the proofs of correctness are however distinct as well as the implementations. For instance, a generic element $L \in \mathcal{K}_{t,\succeq}$ is any element in the relative interior of the cone $\mathcal{K}_{t,\succeq}$ and can be found with appropriate interior-point algorithms for semidefinite programming optimization. On the other hand, a generic element in $\mathcal{K}_t$ can be found using some randomization argument (cf. details later in Section 3.1.4). Moreover, if $L$ is a generic element of $\mathcal{K}_{t,\succeq}$, then $\operatorname{Ker} M_s(L) \subseteq \operatorname{Ker} M_s(L')$ for *all* $L' \in \mathcal{K}_{t,\succeq}$, a property which is not true in general for a generic element $L \in \mathcal{K}_t$ (namely it is not true if the algebra $\mathbb{R}[x]/I$ is not Gorenstein; cf. Section 3.2 for details). For a generic $L \in K_t$ ($K_t = \mathcal{K}_t$ or $\mathcal{K}_{t,\succeq}$), a useful property is that $\operatorname{Ker} M_s(L) \subseteq I(V_{\mathbb{K}}(I))$. This property is true in both cases $\mathbb{K} = \mathbb{R}, \mathbb{C}$. However, while this fact is fairly immediate in the real case, the proof is technically more involved in the complex case (cf. Section 3.1.2). Finally, in the complex case, if the answer is 'yes' in Step 2, we can only claim that the ideal $J := \langle \operatorname{Ker} M_s(L) \rangle$ is nested between $I$ and $I(V_{\mathbb{C}}(I))$; as $V_{\mathbb{C}}(J) = V_{\mathbb{C}}(I)$ this property is however sufficient for the task of computing $V_{\mathbb{C}}(I)$.

Another contribution of the paper is to relate the stopping criteria (1.4) and (1.5) used in our moment based approach to the stopping criterion

$$\dim \pi_s(\mathcal{K}_t) = \dim \pi_{s-1}(\mathcal{K}_t) = \dim \pi_s(\mathcal{K}_{t+1}) \tag{1.6}$$

(where $\pi_s$ denotes the projection from $(\mathbb{R}[x]_t)^*$ onto $(\mathbb{R}[x]_s)^*$) used e.g. in the method of Zhi and Reid [18].

Roughly speaking, if (1.6) holds for some $D \leq s \leq t$, then $\mathbb{R}[x]_s \cap I = \mathbb{R}[x]_s \cap \operatorname{Span}_{\mathbb{R}}(\mathcal{H}_t)$ and one can construct a basis $\mathcal{B} \subseteq \mathbb{R}[x]_{s-1}$ of $\mathbb{R}[x]/I$ (enabling computing $V_{\mathbb{C}}(I)$) (see Section 4.1 for details). Thus the condition (1.6) is a global condition on the set $\mathcal{K}_t$ while (1.4) and (1.5) are conditions on a generic element $L \in \mathcal{K}_t$. However these two types of conditions are closely related as shown in Section 4.2.

**Contents of the paper.** The paper is organized as follows. In Section 2 we introduce some definitions and results about polynomials and moment matrices that we need in the paper. In Section 3 we present our algorithm for computing the complex roots of a zero-dimensional ideal using moment matrices and discuss some small examples. In Section 4 we revisit the involutive base method of Zhi and Reid and compare the various stopping criteria.

## 2. Preliminaries.

In this section we recall some preliminaries of polynomial algebra and moment matrices used throughout the paper.

### 2.1. Some basics of algebraic geometry.

**2.1.1. Polynomial ideals and varieties.** Let $\mathbb{R}[x] := \mathbb{R}[x_1, \ldots, x_n]$ denote the ring of multivariate polynomials in $n$ variables. For $\alpha \in \mathbb{N}^n$, the monomial $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ has degree $|\alpha| := \sum_{i=1}^n \alpha_i$. Set $\mathbb{N}^n_t := \{\alpha \in$

$\mathbb{N}^n \mid |\alpha| \leq t\}$. Then $\mathbb{T}^n := \{x^\alpha \mid \alpha \in \mathbb{N}^n\}$ denotes the set of all monomials in $n$ variables and $\mathbb{T}^n_t := \{x^\alpha \mid \alpha \in \mathbb{N}^n_t\}$ the subset of monomials of degree smaller or equal to $t$. Given polynomials $h_1, \ldots, h_m \in \mathbb{R}[x]$,

$$I = \langle h_1, \ldots, h_m \rangle := \Big\{ \sum_{j=1}^m a_j h_j \mid \quad a_1, \ldots, a_m \in \mathbb{R}[x] \Big\}$$

is the ideal generated by $h_1, \ldots, h_m$. The algebraic variety of $I$ is the set

$$V_{\mathbb{C}}(I) = \{v \in \mathbb{C}^n \mid h_j(v) = 0 \; \forall j = 1, \ldots, m\}$$

of common complex zeros to all polynomials in $I$ and its real variety is $V_{\mathbb{R}}(I) := V_{\mathbb{C}}(I) \cap \mathbb{R}^n$. The ideal $I$ is zero-dimensional when its complex variety $V_{\mathbb{C}}(I)$ is finite. Conversely the vanishing ideal of a subset $V \subseteq \mathbb{C}^n$ is the ideal $I(V) := \{f \in \mathbb{R}[x] \mid f(v) = 0 \; \forall v \in V\}$. For an ideal $I \subseteq \mathbb{R}[x]$, we may also define the ideal

$$\sqrt{I} := \Big\{ f \in \mathbb{R}[x] \; \Big| \quad f^m \in I \;\; \text{for some } m \in \mathbb{N} \setminus \{0\} \Big\},$$

called the radical of $I$, and the ideal

$$\sqrt[\mathbb{R}]{I} := \Big\{ p \in \mathbb{R}[x] \; \Big| \; p^{2m} + \sum_j q_j^2 \in I \;\; \text{for some } q_j \in \mathbb{R}[x], m \in \mathbb{N} \setminus \{0\} \Big\},$$

called the real radical ideal of $I$; $I$ is radical (resp., real radical) if $I = \sqrt{I}$ (resp., $I = \sqrt[\mathbb{R}]{I}$). Obviously $I \subseteq \sqrt{I} \subseteq I(V_{\mathbb{C}}(I))$ and $I \subseteq \sqrt[\mathbb{R}]{I} \subseteq I(V_{\mathbb{R}}(I))$. The relation between vanishing and (real) radical ideals is stated in the following two famous theorems:

THEOREM 2.1. *Let $I \subseteq \mathbb{R}[x]$ be an ideal.*
**(i)** *Hilbert's Nullstellensatz (see, e.g., [3, §4.1]) $\sqrt{I} = I(V_{\mathbb{C}}(I))$.*
**(ii)** *Real Nullstellensatz (see, e.g., [2, §4.1]) $\sqrt[\mathbb{R}]{I} = I(V_{\mathbb{R}}(I))$.*

**2.1.2. The (dual) ring of polynomials.** Given a vector space $A$ on $\mathbb{R}$, its dual space $A^* := \mathrm{Hom}(A, \mathbb{R})$ consists of all linear functionals from $A$ to $\mathbb{R}$. Given a subset $B \subseteq A$, set $B^\perp := \{L \in A^* \mid L(b) = 0 \; \forall b \in B\}$. Then $\mathrm{Span}_{\mathbb{R}}(B) \subseteq (B^\perp)^\perp$, with equality when $A$ is finite dimensional. Here $\mathrm{Span}_{\mathbb{R}}(B) := \{\sum_{i=1}^m \lambda_i b_i \mid \lambda_i \in \mathbb{R}, b_i \in B\}$. We will mostly work here with the vector space $A = \mathbb{R}[x]$ (or subspaces). Examples of linear functionals on $\mathbb{R}[x]$ are the evaluation $p \in \mathbb{R}[x] \mapsto p(v)$ at any $v \in \mathbb{R}^n$ and, given $\alpha \in \mathbb{N}^n$, the differential functional

$$p \in \mathbb{R}[x] \mapsto \partial_\alpha[v](p) := \frac{1}{\prod_{i=1}^n \alpha_i!} \left( \frac{\partial^{|\alpha|}}{\partial x_1^{\alpha_1} \ldots x_n^{\alpha_n}} p \right)(v), \tag{2.1}$$

which evaluates at $v \in \mathbb{R}^n$ the (scaled) derivative of $p$; thus $\partial_0[v](p) = p(v)$ is the linear form that evaluates $p$ at $v$. Note that, for $\alpha, \beta \in \mathbb{N}^n$,

$$\partial_\alpha[0] \left( \prod_{i=1}^n x_i^{\beta_i} \right) = \begin{cases} 1 \text{ if } \alpha = \beta \\ 0 \text{ otherwise} \end{cases} .$$

Therefore the monomial basis $\mathbb{T}^n = \{x^\alpha \mid \alpha \in \mathbb{N}^n\}$ of $\mathbb{R}[x]$ and the basis $\{\partial_\alpha[0] \mid \alpha \in \mathbb{N}^n\}$ of $(\mathbb{R}[x])^*$ are dual bases. Throughout we will mainly use these two canonical bases. In particular, we write a polynomial $p \in \mathbb{R}[x]$ in the form $p = \sum_\alpha p_\alpha x^\alpha$, and $L \in (\mathbb{R}[x])^*$ in the form $L = \sum_\alpha y_\alpha \partial_\alpha[0]$; thus $p_\alpha = \partial_\alpha[0](p)$ and $y_\alpha = L(x^\alpha)$ are the respective coefficients of $p$ and $L$ in the canonical bases and $L(p) = y^T \operatorname{vec}(p) = \sum_\alpha p_\alpha y_\alpha$. Here we let $\operatorname{vec}(p) := (p_\alpha)_\alpha$ denote the vector of coefficients of the polynomial $p$. Finally, given $v \in \mathbb{C}^n$ and $t \in \mathbb{N}$, set $\zeta_v := (v^\alpha)_{\alpha \in \mathbb{N}^n}$ and $\zeta_{t,v} := (v^\alpha)_{\alpha \in \mathbb{N}^n_t}$; thus $\zeta_v = (\partial_0[v](x^\alpha))_\alpha$ is the coordinate sequence of the linear functional $\partial_0[v]$ in the canonical basis of $(\mathbb{R}[x])^*$.

As vector spaces, both $\mathbb{R}[x]$ and its dual $(\mathbb{R}[x])^*$ are infinite dimensional and so for practical computation it is more convenient to work with the finite dimensional subspaces $\mathbb{R}[x]_t = \{p \in \mathbb{R}[x] \mid \deg(p) \leq t\}$ for $t \in \mathbb{N}$. Both vectors spaces $\mathbb{R}[x]_t$ and its dual $(\mathbb{R}[x]_t)^*$ are isomorphic to $\mathbb{R}^{\mathbb{N}^n_t}$, with canonical dual bases $\mathbb{T}^n_t$ and $\{\partial_\alpha[0] \mid \alpha \in \mathbb{N}^n_t\}$, respectively. Given an integer $s \leq t$, we let $\pi_s$ denote the projection from $\mathbb{R}^{\mathbb{N}^n_t}$ onto $\mathbb{R}^{\mathbb{N}^n_s}$, which can thus be interpreted as the projection from $\mathbb{R}[x]_t$ onto $\mathbb{R}[x]_s$, or from $(\mathbb{R}[x]_t)^*$ onto $(\mathbb{R}[x]_s)^*$ depending on the context.

**2.1.3. The quotient algebra.** Given an ideal $I \subseteq \mathbb{R}[x]$, the quotient set $\mathbb{R}[x]/I$ consists of all cosets $[f] := f + I = \{f + q \mid q \in I\}$ for $f \in \mathbb{R}[x]$, i.e. all equivalent classes of polynomials of $\mathbb{R}[x]$ modulo the ideal $I$. The quotient set $\mathbb{R}[x]/I$ is an algebra with addition $[f] + [g] := [f + g]$, scalar multiplication $\lambda[f] := [\lambda f]$ and with multiplication $[f][g] := [fg]$, for $\lambda \in \mathbb{R}$, $f, g \in \mathbb{R}[x]$.

A useful property is that, when $I$ is zero-dimensional (i.e. $|V_\mathbb{C}(I)| < \infty$), then $\mathbb{R}[x]/I$ is a finite-dimensional vector space and the cardinality of $V_\mathbb{C}(I)$ is related to its dimension, as indicated in Theorem 2.2 below.

THEOREM 2.2. *Let $I$ be an ideal in $\mathbb{R}[x]$. Then $|V_\mathbb{C}(I)| < \infty \iff \dim \mathbb{R}[x]/I < \infty$. Moreover, $|V_\mathbb{C}(I)| \leq \dim \mathbb{R}[x]/I$, with equality if and only if $I$ is radical.*

A proof of this theorem and a detailed treatment of the quotient algebra $\mathbb{R}[x]/I$ can be found e.g. in [3], [23].

Assume $|V_\mathbb{C}(I)| < \infty$ and set $N := \dim \mathbb{R}[x]/I$, $|V_\mathbb{C}(I)| \leq N < \infty$. Consider a set $\mathcal{B} := \{b_1, \ldots, b_N\} \subseteq \mathbb{R}[x]$ for which the cosets $[b_1], \ldots, [b_N]$ are pairwise distinct and $\{[b_1], \ldots, [b_N]\}$ is a basis of $\mathbb{R}[x]/I$; by abuse of language we also say that $\mathcal{B}$ itself is a basis of $\mathbb{R}[x]/I$. Then every $f \in \mathbb{R}[x]$ can be written in a unique way as $f = \sum_{i=1}^N c_i b_i + p$, where $c_i \in \mathbb{R}$, $p \in I$; the polynomial $\mathcal{N}_\mathcal{B}(f) := \sum_{i=1}^N c_i b_i$ is called the residue of $f$ modulo $I$, or its *normal form*, with respect to the basis $\mathcal{B}$. In other words, $\operatorname{Span}_\mathbb{R}(\mathcal{B})$ and $\mathbb{R}[x]/I$ are isomorphic vector spaces.

Following Stetter [23], for an ideal $I \subseteq \mathbb{R}[x]$, define its dual space

$$\mathcal{D}[I] := I^\perp = \{L \in (\mathbb{R}[x])^* \mid L(p) = 0 \ \forall p \in I\} \tag{2.2}$$

consisting of all linear functionals vanishing on $I$. Thus $\mathcal{D}[I]$ is isomorphic to $(\mathbb{R}[x]/I)^*$ and, when $I$ is zero-dimensional,

$$\operatorname{Ker}\mathcal{D}[I] := \mathcal{D}[I]^\perp = \{\, p \in \mathbb{R}[x] \;\mid\; L(p) = 0 \;\forall L \in \mathcal{D}[I] \,\} = I.$$

When $I$ is zero-dimensional and radical the sum of the real and imaginary parts of the evaluation at points $v \in V_{\mathbb{C}}(I)$ form a basis of $\mathcal{D}[I]$; that is,

$$\mathcal{D}[I] = \operatorname{Span}_{\mathbb{R}} \{\operatorname{Re}\partial_0[v] + \operatorname{Im}\partial_0[v] \mid v \in V_{\mathbb{C}}(I)\}\ . \tag{2.3}$$

Indeed, each linear map $\operatorname{Re}\partial_0[v] + \operatorname{Im}\partial_0[v]$ $(v \in V_{\mathbb{C}}(I))$ vanishes at all $p \in I$ and thus belongs to $\mathcal{D}[I]$; moreover, they are linearly independent and $\dim \mathcal{D}[I] = \dim(\mathbb{R}[x]/I)^* = \dim \mathbb{R}[x]/I$, which is equal to $|V_{\mathbb{C}}(I)|$ since $I$ is zero-dimensional and radical (using Theorem 2.2).

**2.1.4. Multiplication operators.** Given a polynomial $h \in \mathbb{R}[x]$, we can define the *multiplication (by $h$) operator* as

$$\begin{array}{rccc} \mathcal{X}_h : & \mathbb{R}[x]/I & \longrightarrow & \mathbb{R}[x]/I \\ & [f] & \longmapsto & \mathcal{X}_h([f]) := [hf]\,, \end{array} \tag{2.4}$$

with adjoint operator

$$\begin{array}{rccc} \mathcal{X}_h^\dagger : & (\mathbb{R}[x]/I)^* & \longrightarrow & (\mathbb{R}[x]/I)^* \\ & L & \longmapsto & L \circ \mathcal{X}_h. \end{array}$$

Assume that $N := \dim \mathbb{R}[x]/I < \infty$. Then the multiplication operator $\mathcal{X}_h$ can be represented by its matrix, again denoted $\mathcal{X}_h$ for simplicity, with respect to a given basis $\mathcal{B} = \{b_1, \ldots, b_N\}$ of $\mathbb{R}[x]/I$ and then $\mathcal{X}_h^T$ represents $\mathcal{X}_h^\dagger$ with respect to the dual basis of $\mathcal{B}$. Namely, setting $\mathcal{N}_{\mathcal{B}}(hb_j) := \sum_{i=1}^N a_{ij} b_i$ for some scalars $a_{ij} \in \mathbb{R}$, the $j$th column of $\mathcal{X}_h$ is the vector $(a_{ij})_{i=1}^N$. Given $v \in \mathbb{C}^n$, define the vector $\zeta_{\mathcal{B},v} := (b_j(v))_{j=1}^N \in \mathbb{C}^N$, whose coordinates are the evaluations at $v$ of the polynomials in $\mathcal{B}$. The following famous result (see e.g. [4, Chapter 2§4]) relates the eigenvalues of the multiplication operators in $\mathbb{R}[x]/I$ to the algebraic variety $V_{\mathbb{C}}(I)$. This result underlies the so-called eigenvalue method for solving polynomial equations and plays a central role in many algorithms, also in the present paper.

THEOREM 2.3. *Let $I$ be a zero-dimensional ideal in $\mathbb{R}[x]$, $\mathcal{B}$ a basis of $\mathbb{R}[x]/I$, and $h \in \mathbb{R}[x]$. The eigenvalues of the multiplication operator $\mathcal{X}_h$ are the evaluations $h(v)$ of the polynomial $h$ at the points $v \in V_{\mathbb{C}}(I)$. Moreover, $(\mathcal{X}_h)^T \zeta_{\mathcal{B},v} = h(v)\zeta_{\mathcal{B},v}$ for all $v \in V_{\mathbb{C}}(I)$.*

Throughout the paper we also denote by $\mathcal{X}_i := \mathcal{X}_{x_i}$ the matrix of the multiplication operator by the variable $x_i$. By the above theorem, the eigenvalues of the matrices $\mathcal{X}_i$ are the $i$th coordinate of the points $v \in V_{\mathbb{C}}(I)$. Thus the task of solving a system of polynomial equations is reduced to a task of numerical linear algebra once a basis of $\mathbb{R}[x]/I$ and a normal form algorithm are available, permitting the construction of the multiplication matrices $\mathcal{X}_i$.

**2.1.5. Normal form criterion.** The eigenvalue method for solving polynomial equations (recall Theorem 2.3) requires knowledge of a basis of $\mathbb{R}[x]/I$ and an algorithm to compute the normal form of a polynomial with respect to this basis. This, in turn, permits the construction of multiplication matrices $\mathcal{X}_i$ $(i = 1, \ldots, n)$ and therefore the computation of $V_{\mathbb{C}}(I)$.

A well known basis of $\mathbb{R}[x]/I$ is the set of standard monomials with respect to some monomial ordering. A classical way to obtain this basis is to compute a Gröbner basis of $I$ from which the normal form of a polynomial can be found via a polynomial division algorithm using the given monomial ordering. (See e.g. [3, Chapter 1] for details.) Other techniques have been proposed for producing bases of the ideal $I$ and of the vector space $\mathbb{R}[x]/I$, which do not depend on a specific monomial ordering. In particular, algorithms have been proposed for constructing border bases of $I$ leading to general (stable by division) bases of $\mathbb{R}[x]/I$ (see [6, Chapter 4], [8] and [23]). Another normal form algorithm is proposed by Mourrain [14] (see also [15, 17]) leading to more general (namely, connected to 1) bases of $\mathbb{R}[x]/I$. The moment-matrix approach of this paper allows the computation of general polynomial bases of $\mathbb{R}[x]/I$ (or of $\mathbb{R}[x]/I(V_{\mathbb{R}}(I))$ as explained in [10]). We now recall the main notions and results about *border bases* and *rewriting families* needed for our treatment, following mainly [15, 17].

Definition 2.1. *Given $\mathcal{B} \subseteq \mathbb{T}^n$, let $\mathcal{B}^+ = \mathcal{B} \cup x_1\mathcal{B} \cup x_2\mathcal{B} \cup \ldots \cup x_n\mathcal{B}$ with $x_i\mathcal{B} := \{x_i b \mid b \in \mathcal{B},\ i = 1, \ldots, n\}$, the expansion of $\mathcal{B}$ with one degree, and $\partial\mathcal{B} := \mathcal{B}^+ \setminus \mathcal{B}$, the border set of $\mathcal{B}$. The set $\mathcal{B}$ is said to be* connected to 1 *if each $m \in \mathcal{B}$ can be written as $m = m_1 \cdots m_t$ with $m_1 = 1$ and $m_1 \cdots m_s \in \mathcal{B}$ $(s = 1, \ldots, t)$. Moreover, $\mathcal{B} \subseteq \mathbb{T}^n$ is said to be* stable by division *if, for all $m, m' \in \mathcal{B}$,*

$$m \in \mathcal{B},\ m'|m \Rightarrow m' \in \mathcal{B}.$$

*Obviously, $\mathcal{B}$ is connected to 1 if it is stable by division.*

Assume $\mathcal{B} \subseteq \mathbb{T}^n$ is connected to 1. For each monomial $m \in \partial\mathcal{B}$, consider a polynomial $f_m$ of the form

$$f_m := m - r_m \quad \text{where } r_m := \sum_{b \in \mathcal{B}} \lambda_{m,b}\, b \in \mathrm{Span}_{\mathbb{R}}(\mathcal{B}) \quad (\lambda_{m,b} \in \mathbb{R}). \tag{2.5}$$

The family

$$F := \{f_m \mid m \in \partial\mathcal{B}\}$$

is called a *rewriting family for* $\mathcal{B}$ in [15, 17] (or a $\mathcal{B}$-border prebasis in [6, Chapter 4]; note that $\mathcal{B}$ is assumed to be stable by division there). Thus a rewriting family enables expressing all monomials in $\partial\mathcal{B}$ as linear combinations of monomials in $\mathcal{B}$ modulo the ideal $\langle F \rangle$. Such a rewriting family can be used in a polynomial division algorithm to decompose any polynomial $p \in \mathbb{R}[x]$ as

$$p = r_p + \sum_{m \in \partial\mathcal{B}} u_m f_m \quad \text{where } r_p \in \mathrm{Span}_{\mathbb{R}}(\mathcal{B}),\ u_m \in \mathbb{R}[x]. \tag{2.6}$$

Therefore the set $\mathcal{B}$ spans the vector space $\mathbb{R}[x]/\langle F\rangle$ and in addition, if $\mathcal{B}$ is linearly independent in $\mathbb{R}[x]/\langle F\rangle$ then $\mathcal{B}$ is a basis of $\mathbb{R}[x]/\langle F\rangle$. This latter condition is equivalent to requiring that any polynomial can be reduced in a unique way using the rewriting family $F$ and thus the decomposition (2.6) does not depend on the order in which the rewriting rules taken from $F$ are applied.

Formally we can define a linear operator $\mathcal{X}_i : \mathrm{Span}_{\mathbb{R}}(\mathcal{B}) \to \mathrm{Span}_{\mathbb{R}}(\mathcal{B})$ using the rewriting family $F$; namely, for $b \in \mathcal{B}$, $\mathcal{X}_i(b) := x_i b$ if $x_i b \in \mathcal{B}$ and $\mathcal{X}_i(b) := N_{\mathcal{B}}(x_i b) = x_i b - f_{x_i b} = r_{x_i b}$ otherwise (recall (2.5)), and extend $\mathcal{X}_i$ to $\mathrm{Span}_{\mathbb{R}}(\mathcal{B})$ by linearity. Denote also by $\mathcal{X}_i$ the matrix of this linear operator, which can be seen as a *formal multiplication (by $x_i$) matrix*. The next result shows that the pairwise commutativity of the $\mathcal{X}_i$'s is sufficient to ensure the uniqueness of a decomposition (2.6). (See also [6, Chapter 4] in the case when $\mathcal{B}$ is stable by division.)

THEOREM 2.4. *[14] Let $\mathcal{B} \subseteq \mathbb{T}^n$ be a set connected to 1, let $F$ be a rewriting family for $\mathcal{B}$, with associated formal multiplication matrices $\mathcal{X}_1, \ldots, \mathcal{X}_n$, and let $J := \langle F\rangle$ be the ideal generated by $F$. The following conditions are equivalent.*
**(i)** *The matrices $\mathcal{X}_1, \ldots, \mathcal{X}_n$ commute pairwise.*
**(ii)** *$\mathbb{R}[x] = \mathrm{Span}_{\mathbb{R}}(\mathcal{B}) \oplus J$, i.e. $\mathcal{B}$ is a basis of $\mathbb{R}[x]/J$.*
*Then $F$ is called a* border basis *of the ideal $J$, and the matrix $\mathcal{X}_i$ represents the multiplication operator $m_{x_i}$ of $\mathbb{R}[x]/J$ with respect to the basis $\mathcal{B}$.*

### 2.2. Bilinear forms and moment matrices.

**2.2.1. Bilinear forms.** Given $L \in (\mathbb{R}[x])^*$, we can define the symmetric bilinear form on $\mathbb{R}[x]$

$$\begin{aligned}(\cdot,\cdot)_L : \mathbb{R}[x] \times \mathbb{R}[x] &\to \mathbb{R}\\ (f,g) &\mapsto (f,g)_L := L(fg)\end{aligned}$$

with associated quadratic form

$$\begin{aligned}(\cdot)_L : \mathbb{R}[x] &\to \mathbb{R}\\ f &\mapsto \quad (f)_L := (f,f)_L = L(f^2).\end{aligned}$$

The kernel of this bilinear form $(\cdot,\cdot)_L$ is an ideal of $\mathbb{R}[x]$ (see e.g. [5]), which is real radical whenever the quadratic form $(\cdot)_L$ is positive semidefinite, i.e. satisfies $(f)_L = L(f^2) \geq 0$ for all $f \in \mathbb{R}[x]$ (see [12], [13]). We can define truncated analogues of $(\cdot,\cdot)_L$ and $(\cdot)_L$ on $\mathbb{R}[x]_t$ in the following way. Given $L \in (\mathbb{R}[x]_t)^*$, consider the bilinear form on $\mathbb{R}[x]_{\lfloor t/2\rfloor}$

$$\begin{aligned}(\cdot,\cdot)_L : \mathbb{R}[x]_{\lfloor t/2\rfloor} \times \mathbb{R}[x]_{\lfloor t/2\rfloor} &\to \mathbb{R}\\ (f,g) &\mapsto \quad (f,g)_L := L(fg)\,,\end{aligned}$$

with associated quadratic form $(\cdot)_L$ on $\mathbb{R}[x]_{\lfloor t/2 \rfloor}$ defined by $(f)_L := L(f^2)$ for $f \in \mathbb{R}[x]_{\lfloor t/2 \rfloor}$.

**2.2.2. Moment matrices.** Fixing the canonical basis $(x^\alpha)_\alpha$ of the polynomial ring, the quadratic form $(\cdot)_L$ is positive semidefinite precisely when the matrix $(L(x^{\alpha+\beta}))_{\alpha,\beta}$ (with rows and columns indexed by $\mathbb{N}^n$ when $L \in (\mathbb{R}[x])^*$, and by $\mathbb{N}^n_{\lfloor t/2 \rfloor}$ when $L \in (\mathbb{R}[x]_t)^*$) is positive semidefinite. Note that the $(\alpha, \beta)$-entry of this matrix depends only on the sum $\alpha + \beta$ and such a matrix is also known as the *moment matrix* associated with $L$. We may identify $L \in (\mathbb{R}[x])^*$ with its coordinate sequence $y := (L(x^\alpha))_{\alpha \in \mathbb{N}^n}$ in the canonical basis of $(\mathbb{R}[x])^*$, in which case we also write $L = L_y$.

Given $y \in \mathbb{R}^{\mathbb{N}^n}$, let $M(y)$ denote the matrix with rows and columns indexed by $\mathbb{N}^n$, and with $(\alpha, \beta)$-entry $y_{\alpha+\beta}$, known as the *moment matrix* of $y$ (or of the associated linear functional $L_y$). Analogously, for $L \in (\mathbb{R}[x]_t)^*$, let $y := (L(x^\alpha))_{\alpha \in \mathbb{N}^n_t}$ be the coordinate sequence of $L$ in the canonical basis of $(\mathbb{R}[x]_t)^*$ and define the (truncated) moment matrix $M_{\lfloor t/2 \rfloor}(y)$ with rows and columns indexed by $\mathbb{N}^n_{\lfloor t/2 \rfloor}$, and with $(\alpha, \beta)$-entry $y_{\alpha+\beta}$. Then $(\cdot)_L$ is positive semidefinite if and only if the matrix $M_{\lfloor t/2 \rfloor}(y)$ is positive semidefinite.

The kernel of $M(y)$ (resp. $M_{\lfloor t/2 \rfloor}(y)$) can be identified with the set of polynomials $p \in \mathbb{R}[x]$ (resp. $p \in \mathbb{R}[x]_{\lfloor t/2 \rfloor}$) such that $M(y)\,\mathrm{vec}(p) = 0$ (resp. $M_{\lfloor t/2 \rfloor}(y)\,\mathrm{vec}(p) = 0$). As observed above, $\mathrm{Ker}\, M(y)$ is an ideal of $\mathbb{R}[x]$ (and so $\mathrm{Ker}\, M(y) = \langle \mathrm{Ker}\, M(y) \rangle$), which is real radical when $M(y) \succeq 0$.

For $L := \partial_0[v]$, the evaluation at $v \in \mathbb{R}^n$, the quadratic form $(\cdot)_L$ is obviously positive semidefinite. Moreover, as the coordinate sequence of $L$ in the canonical basis of $(\mathbb{R}[x])^*$ is $\zeta_v = (v^\alpha)_\alpha$, the matrix associated with $(\cdot)_L$ is just $\zeta_v \zeta_v^T$, and its kernel is the set of polynomials $p \in \mathbb{R}[x]$ that vanish at the point $v$. The above features explain the relevance of positive semidefinite quadratic forms and moment matrices to the problem of computing the real solutions of a system of polynomial equations. In [10] the 'real radical ideal' property of the kernel of a positive semidefinite quadratic form played a central role for finding all real roots and the real radical ideal for a zero-dimensional ideal of $\mathbb{R}[x]$. Here we will extend the method of [10] and show that, without the positive semidefiniteness assumption, bilinear forms and moment matrices can still be used for finding all complex roots of zero-dimensional systems of polynomial equations.

**2.2.3. Flat extensions of moment matrices.** We recall here some results about moment matrices needed throughout. We begin with recalling the following elementary property of kernels of block matrices, used for flat extensions of moment matrices in Theorems 2.5, 2.6 below.

LEMMA 2.1. *Let* $M = \begin{pmatrix} A & B \\ B^T & C \end{pmatrix}$ *be a symmetric matrix.*

**(i)** *Assume* $\operatorname{rank} M = \operatorname{rank} A$. *Then,* $x \in \operatorname{Ker} A \iff \tilde{x} := \begin{pmatrix} x \\ 0 \end{pmatrix} \in \operatorname{Ker} M$ *and* $\operatorname{Ker} M = \operatorname{Ker} \begin{pmatrix} A & B \end{pmatrix}$.

**(ii)** *Assume* $M \succeq 0$. *Then,* $x \in \operatorname{Ker} A \iff \tilde{x} := \begin{pmatrix} x \\ 0 \end{pmatrix} \in \operatorname{Ker} M$.

*Proof.* (i) As $\operatorname{rank} M = \operatorname{rank} A$, there exists a matrix $U$ for which $B = AU$ and $C = B^T U = U^T AU$. Then, $Ax = 0 \Longrightarrow B^T x = U^T Ax = 0 \Longrightarrow M\tilde{x} = 0$. Moreover, $Ax + By = 0$ implies $By = -Ax$ and thus $B^T x + Cy = U^T Ax + U^T AUy = U^T Ax + U^T(-Ax) = 0$, showing (i).

(ii) If $Ax = 0$ then $\tilde{x}^T M\tilde{x} = x^T Ax = 0$, which implies $M\tilde{x} = 0$ when $M \succeq 0$. □

When a matrix $M$ with the block form shown in Lemma 2.1 satisfies $\operatorname{rank} M = \operatorname{rank} A$, one says that $M$ *is a flat extension of* $A$. Curto and Fialkow [5] show the following result (see also [11] for a detailed exposition).

THEOREM 2.5. *[5] (Flat Extension theorem) Let* $y \in \mathbb{R}^{\mathbb{N}^n_{2t}}$ *and assume that*

$$\operatorname{rank} M_t(y) = \operatorname{rank} M_{t-1}(y).$$

*Then one can extend* $y$ *to* $\tilde{y} \in \mathbb{R}^{\mathbb{N}^n_{2t+2}}$ *in such a way that* $\operatorname{rank} M_{t+1}(\tilde{y}) = \operatorname{rank} M_t(y)$.

Based on this, one can prove the following result which plays a central role in our moment-matrix approach (as well as in the previous paper [10]).

THEOREM 2.6. *Let* $y \in \mathbb{R}^{\mathbb{N}^n_{2t}}$ *and assume that*

$$\operatorname{rank} M_t(y) = \operatorname{rank} M_{t-1}(y).$$

*Then one can extend* $y$ *to* $\tilde{y} \in \mathbb{R}^{\mathbb{N}^n}$ *in such a way that* $\operatorname{rank} M(\tilde{y}) = \operatorname{rank} M_t(y)$. *Moreover,* $\operatorname{Ker} M(\tilde{y}) = \langle \operatorname{Ker} M_t(y) \rangle$, *and any basis* $\mathcal{B} \subseteq \mathbb{T}^n_{t-1}$ *of the column space of* $M_t(y)$ *is a basis of* $\mathbb{R}[x]/\langle \operatorname{Ker} M(\tilde{y}) \rangle$.

*Proof.* The existence of $\tilde{y}$ follows applying iteratively Theorem 2.5. As $\operatorname{rank} M(\tilde{y}) = \operatorname{rank} M_t(y)$, the inclusion $\operatorname{Ker} M_t(y) \subseteq \operatorname{Ker} M(\tilde{y})$ follows from Lemma 2.1 (i). Hence $\langle \operatorname{Ker} M_t(y) \rangle \subseteq \operatorname{Ker} M(\tilde{y})$, since $\operatorname{Ker} M(\tilde{y})$ is an ideal of $\mathbb{R}[x]$. Let $\mathcal{B} \subseteq \mathbb{T}^n_{t-1}$ index a basis of the column space of $M_t(y)$. Hence $\mathcal{B}$ also indexes a basis of the column space of $M(\tilde{y})$, which implies $\operatorname{Span}_{\mathbb{R}}(\mathcal{B}) \cap \operatorname{Ker} M(\tilde{y}) = \{0\}$ and thus $\operatorname{Span}_{\mathbb{R}}(\mathcal{B}) \cap \langle \operatorname{Ker} M_t(y) \rangle = \{0\}$. We now show that

$$\mathbb{R}[x] = \operatorname{Span}_{\mathbb{R}}(\mathcal{B}) \oplus \langle \operatorname{Ker} M_t(y) \rangle. \tag{2.7}$$

For this it suffices to show that $x^\alpha \in \operatorname{Span}_{\mathbb{R}}(\mathcal{B}) + \langle \operatorname{Ker} M_t(y) \rangle$ for all $\alpha \in \mathbb{N}^n$. We use induction on $|\alpha|$. If $|\alpha| \leq t$ just use the definition of $\mathcal{B}$. Next, let $|\alpha| \geq t+1$ and write $x^\alpha = x_i x^\delta$. By the induction assumption, $x^\delta = \sum_{x^\beta \in \mathcal{B}} \lambda_\beta x^\beta + q$ where $q \in \langle \operatorname{Ker} M_t(y) \rangle$. Hence, $x^\alpha = \sum_{x^\beta \in \mathcal{B}} \lambda_\beta x_i x^\beta +$

$x_i q$, with $x_i q \in \langle \operatorname{Ker} M_t(y)\rangle$. As $\deg(x_i x^\beta) \le 1 + t - 1 = t$, each $x_i x^\beta$ lies in $\operatorname{Span}_{\mathbb{R}}(\mathcal{B}) + \langle \operatorname{Ker} M_t(y)\rangle$ and therefore $x^\alpha$ also lies in $\operatorname{Span}_{\mathbb{R}}(\mathcal{B}) + \langle \operatorname{Ker} M_t(y)\rangle$. Hence (2.7) holds. This implies

$$\operatorname{Ker} M(\tilde{y}) = \langle \operatorname{Ker} M_t(y)\rangle.$$

Indeed let $f \in \operatorname{Ker} M(\tilde{y})$ and write $f = r + q$ with $r \in \operatorname{Span}_{\mathbb{R}}(\mathcal{B})$ and $q \in \langle \operatorname{Ker} M_t(y)\rangle$. Thus $r = f - q \in \operatorname{Ker} M(\tilde{y}) \cap \operatorname{Span}_{\mathbb{R}}(\mathcal{B}) = \{0\}$, which implies $f = q \in \langle \operatorname{Ker} M_t(y)\rangle$. The above argument also shows that $\mathcal{B}$ is a basis of the space $\mathbb{R}[x]/\langle \operatorname{Ker} M_t(y)\rangle$. □

**3. The moment-matrix approach for complex roots.** In this section we show how the method from [10] can be simply adapted to find all complex roots for a zero-dimensional ideal. The method of [10] was designed to find $V_{\mathbb{R}}(I)$ (assuming it is finite) and uses the set $K_{t,\succeq}$ introduced in (1.3). We now show that only by *omitting* the positivity condition in (1.3) and working instead with the set $\mathcal{K}_t$ from (1.2), we can find the complex variety $V_{\mathbb{C}}(I)$.

**3.1. Approaching $I$ with kernels of moment matrices.** Let $I = \langle h_1, \dots, h_m\rangle$ be a zero-dimensional ideal whose associated complex variety $V_{\mathbb{C}}(I)$ has to be found. Throughout we set

$$D := \max_{j=1,\dots,m} \deg(h_j), \quad d := \max_{j=1,\dots,m} \lceil \deg(h_j)/2 \rceil = \lceil D/2 \rceil. \tag{3.1}$$

Recall the definition of the sets $\mathcal{H}_t$, $\mathcal{K}_t$ from (1.1), (1.2):

$$\mathcal{H}_t := \{x^\alpha h_j \in \mathbb{R}[x]_t \mid j = 1, \dots, m,\ \alpha \in \mathbb{N}^n \ \text{ with } |\alpha| + \deg(h_j) \le t\},$$

$$\mathcal{K}_t = \mathcal{H}_t^\perp = \{L \in (\mathbb{R}[x]_t)^* \mid L(p) = 0 \quad \forall p \in \mathcal{H}_t\}.$$

Equivalently, identifying $L \in (\mathbb{R}[x]_t)^*$ with its sequence of coefficients $y = (y_\alpha)_\alpha$ in the canonical basis of $(\mathbb{R}[x]_t)^*$ and setting $L_y := L$,

$$\mathcal{K}_t = \{y \in \mathbb{R}^{\mathbb{N}_t^n} \mid L_y(p) = y^T \operatorname{vec}(p) = 0 \quad \forall p \in \mathcal{H}_t\}.$$

For further reference, notice the following fact about the moment matrix $M_{\lfloor t/2\rfloor}(y)$ of an arbitrary $y \in \mathbb{R}^{\mathbb{N}_t^n}$. If $\deg(fg),\ \deg(gh) \le \lfloor t/2\rfloor$ then

$$\operatorname{vec}(f)^T M_{\lfloor t/2\rfloor}(y) \operatorname{vec}(gh) = \operatorname{vec}(fg)^T M_{\lfloor t/2\rfloor}(y) \operatorname{vec}(h)\ (= L_y(fgh)). \tag{3.2}$$

We now show several results relating the kernel of the moment matrix $M_{\lfloor t/2\rfloor}(y)$ of $y \in \mathcal{K}_t$ to the ideal $I$.

**3.1.1. The inclusion $I \subseteq \langle \operatorname{Ker} M_{\lfloor t/2\rfloor}(y)\rangle$.** The next two lemmas give sufficient conditions ensuring that the ideal generated by the kernel of $M_{\lfloor t/2\rfloor}(y)$ contains the ideal $I$.

LEMMA 3.1. *Let $y \in \mathcal{K}_t$ and let $s$ be an integer with $D \le s \le \lfloor t/2 \rfloor$. Then $\mathrm{vec}(h_1), \ldots, \mathrm{vec}(h_m) \in \mathrm{Ker}\, M_s(y)$ and thus $I \subseteq \langle \mathrm{Ker}\, M_s(y) \rangle$.*

*Proof.* For $\alpha \in \mathbb{N}^n_s$, $(M_s(y)\,\mathrm{vec}(h_j))_\alpha = L_y(x^\alpha h_j) = 0$ since $x^\alpha h_j \in \mathcal{H}_t$ as $\deg(x^\alpha h_j) \le s + D \le t$. ∎

LEMMA 3.2. *Let $y \in \mathcal{K}_t$ and let $s$ be an integer with $d \le s \le \lfloor t/2 \rfloor$. If $\mathrm{rank}\, M_s(y) = \mathrm{rank}\, M_{s-d}(y)$ then $I \subseteq \langle \mathrm{Ker}\, M_s(y) \rangle$.*

*Proof.* We apply Theorem 2.6: Let $\tilde{y} \in \mathbb{R}^{\mathbb{N}^n}$ be an extension of $\pi_{2s}(y)$ such that $\mathrm{rank}\, M(\tilde{y}) = \mathrm{rank}\, M_s(y)$ and let $\mathcal{B} \subseteq \mathbb{T}^n_{s-d}$ index a basis of the column space of $M_s(y)$. Then $\mathcal{B}$ is a basis of $\mathbb{R}[x]/\,\mathrm{Ker}\, M(\tilde{y})$ and $\mathrm{Ker}\, M(\tilde{y}) = \langle \mathrm{Ker}\, M_s(y) \rangle$. It suffices now to show that $h_j \in \mathrm{Ker}\, M(\tilde{y})$ for all $j = 1, \ldots, m$. For this write $h_j = r + q$ where $r \in \mathrm{Span}_{\mathbb{R}}(\mathcal{B})$ and $q \in \mathrm{Ker}\, M(\tilde{y})$. Then $M(\tilde{y})\,\mathrm{vec}(h_j) = M(\tilde{y})\,\mathrm{vec}(r)$. As $\deg(r) \le s-d$ and $M(\tilde{y})$ is a flat extension of $M_{s-d}(\tilde{y})$, Lemma 2.1 (i) implies that $M(\tilde{y})\,\mathrm{vec}(r) = 0$ if and only if $M_{s-d}(\tilde{y})\,\mathrm{vec}(r) = 0$, i.e. $\mathrm{vec}(x^\alpha)^T M(\tilde{y})\,\mathrm{vec}(r) = 0$ for all $\alpha \in \mathbb{N}^n_{s-d}$. Given $\alpha \in \mathbb{N}^n_{s-d}$, $\mathrm{vec}(x^\alpha)^T M(\tilde{y})\,\mathrm{vec}(r) = \mathrm{vec}(x^\alpha)^T M(\tilde{y})\,\mathrm{vec}(h_j) = L_{\tilde{y}}(x^\alpha h_j)$, which is equal to $L_y(x^\alpha h_j)$ since $\deg(x^\alpha h_j) \le s - d + 2d \le 2s$, and in turn is equal to 0 since $x^\alpha h_j \in \mathcal{H}_t$ and $y \in \mathcal{K}_t$. ∎

**3.1.2. The inclusion $\langle \mathrm{Ker}\, M_t(y) \rangle \subseteq I(V_{\mathbb{C}}(I))$ for generic $y$.** We now show that, under some maximality assumption on the rank of the matrix $M_{\lfloor t/2 \rfloor}(y)$, the polynomial ideal $\langle \mathrm{Ker}\, M_{\lfloor t/2 \rfloor}(y) \rangle$ is contained in $I(V_{\mathbb{C}}(I))$.

THEOREM 3.1. *Given $1 \le s \le \lfloor t/2 \rfloor$, let $y \in \mathcal{K}_t$ for which $\mathrm{rank}\, M_s(y)$ is maximum; that is,*

$$\mathrm{rank}\, M_s(y) = \max_{z \in \mathcal{K}_t} \mathrm{rank}\, M_s(z). \tag{3.3}$$

*Then $\langle \mathrm{Ker}\, M_s(y) \rangle \subseteq I(V_{\mathbb{C}}(I))$.*

*Proof.* It suffices to show that $\mathrm{Ker}\, M_s(y) \subseteq I(V_{\mathbb{C}}(I))$. Suppose for contradiction that there exists $f \in \mathbb{R}[x]_s$ with $\mathrm{vec}(f) \in \mathrm{Ker}\, M_s(y)$ and $f \notin I(V_{\mathbb{C}}(I))$. Then there exists $v \in V_{\mathbb{C}}(I)$ for which $f(v) \neq 0$.

We first consider the case when $v \in \mathbb{R}^n$. Then $\zeta_{t,v} \in \mathcal{K}_t$. Set $y' := y + \zeta_{t,v}$. Then $y' \in \mathcal{K}_t$ and $\mathrm{vec}(f) \notin \mathrm{Ker}\, M_s(y')$ since $\mathrm{vec}(f) \notin \mathrm{Ker}\, M_s(\zeta_{t,v})$. Therefore, $\mathrm{Ker}\, M_s(y') \not\subseteq \mathrm{Ker}\, M_s(y)$, for otherwise we would have strict inclusion: $\mathrm{Ker}\, M_s(y') \subsetneq \mathrm{Ker}\, M_s(y)$, implying $\mathrm{rank}\, M_s(y') > \mathrm{rank}\, M_s(y)$ and thus contradicting the maximality assumption on $\mathrm{rank}\, M_s(y)$. Hence there exists $f' \in \mathbb{R}[x]_s$ with $\mathrm{vec}(f') \in \mathrm{Ker}\, M_s(y') \setminus \mathrm{Ker}\, M_s(y)$. We have $M_s(y)\,\mathrm{vec}(f') = -f'(v)\zeta_{s,v}$ and $f'(v) \neq 0$. Moreover,

$$\mathrm{vec}(f)^T M_s(y)\,\mathrm{vec}(f') = -f(v)f'(v)\,,$$

yielding a contradiction since $f(v)f'(v) \neq 0$ and $\mathrm{vec}(f)^T M_s(y)\,\mathrm{vec}(f') = 0$.

We now consider the case when $v \in \mathbb{C}^n \setminus \mathbb{R}^n$. The proof is along the same lines but needs a more detailed analysis. We start with the following observation.

CLAIM 3.2. *For $v \in \mathbb{C}^n \setminus \mathbb{R}^n$ and $s \geq 1$, the two vectors $\zeta_{s,v}$ and $\zeta_{s,\overline{v}}$ are linearly independent over $\mathbb{C}$.*

*Proof.* Assume $\lambda\zeta_{s,v} + \mu\zeta_{s,\overline{v}} = 0$ where $\lambda, \mu \in \mathbb{C}$. Then $\lambda + \mu = 0$ (evaluating at the coordinate indexed by the constant monomial 1) and $\lambda(v_i - \overline{v}_i) = 0$ $(i = 1, \ldots, n)$, implying $\lambda = \mu = 0$ since $v_i \notin \mathbb{R}$ for some $i$. □

Define the two vectors

$$y' := y + f(\overline{v})\zeta_{t,v} + f(v)\zeta_{t,\overline{v}},\ y'' := y + \mathbf{i}(f(v)\zeta_{t,\overline{v}} - f(\overline{v})\zeta_{t,v}),$$

where $\mathbf{i}$ denotes the complex root of $-1$. Then, $y', y'' \in \mathcal{K}_t$, $\operatorname{vec}(f) \notin \operatorname{Ker} M_s(y')$ since $M_s(y')\operatorname{vec}(f) = |f(v)|^2(\zeta_{s,v} + \zeta_{s,\overline{v}}) \neq 0$ and $\operatorname{vec}(f) \notin \operatorname{Ker} M_s(y'')$ since $M_s(y'')\operatorname{vec}(f) = \mathbf{i}|f(v)|^2(\zeta_{s,\overline{v}} - \zeta_{s,v}) \neq 0$ (as $v \notin \mathbb{R}^n$). By the maximality assumption on $\operatorname{rank} M_s(y)$, $\operatorname{Ker} M_s(y') \not\subset \operatorname{Ker} M_s(y)$ and $\operatorname{Ker} M_s(y'') \not\subset \operatorname{Ker} M_s(y)$. In what follows, $\operatorname{Re} a$, $\operatorname{Im} a$ denote, respectively, the real and imaginary parts of $a \in \mathbb{C}$.

CLAIM 3.3.
**(i)** $\operatorname{Re} g(v) = 0$ *for all* $g \in \mathbb{R}[x]_s$ *with* $\operatorname{vec}(g) \in \operatorname{Ker} M_s(y') \setminus \operatorname{Ker} M_s(y)$.
**(ii)** $\operatorname{Im} g(v) = 0$ *for all* $g \in \mathbb{R}[x]_s$ *with* $\operatorname{vec}(g) \in \operatorname{Ker} M_s(y'') \setminus \operatorname{Ker} M_s(y)$.

*Proof.* (i) For $g \in \mathbb{R}[x]_s$ with $\operatorname{vec}(g) \in \operatorname{Ker} M_s(y')$, we have:

$$\begin{aligned} 0 &= \operatorname{vec}(f)^T M_s(y')\operatorname{vec}(g) \\ &= \operatorname{vec}(f)^T(f(\overline{v})\zeta_{s,v}\zeta_{s,v}^T + f(v)\zeta_{s,\overline{v}}\zeta_{s,\overline{v}}^T)\operatorname{vec}(g) \\ &= |f(v)|^2(g(v) + g(\overline{v})) \end{aligned}$$

implying that $g(v)$ is a pure imaginary complex number, i.e., $\operatorname{Re} g(v) = 0$.
(ii) Similarly, for $g \in \mathbb{R}[x]_s$ with $\operatorname{vec}(g) \in \operatorname{Ker} M_s(y'')$,

$$0 = \operatorname{vec}(f)^T M_s(y'')\operatorname{vec}(g) = \mathbf{i}|f(v)|^2(g(\overline{v}) - g(v))$$

which implies that $g(v) \in \mathbb{R}$, i.e., $\operatorname{Im} g(v) = 0$. □

Fix $f' \in \mathbb{R}[x]_s$ with $\operatorname{vec}(f') \in \operatorname{Ker} M_s(y') \setminus \operatorname{Ker} M_s(y)$ and fix $f'' \in \mathbb{R}[x]_s$ with $\operatorname{vec}(f'') \in \operatorname{Ker} M_s(y'') \setminus \operatorname{Ker} M_s(y)$ with $f'(v) = \mathbf{i}$ and $f''(v) = 1$. Set $W_0' := \operatorname{Ker} M_s(y) \cap \operatorname{Ker} M_s(y')$.

CLAIM 3.4.
**(i)** $\operatorname{Ker} M_s(y') = W_0' + \mathbb{R}\operatorname{vec}(f')$.
**(ii)** $\operatorname{Ker} M_s(y) = W_0' + \mathbb{R}\operatorname{vec}(f)$.
**(iii)** $g(v) = 0$ *for all* $g \in \mathbb{R}[x]_s$ *with* $\operatorname{vec}(g) \in W_0'$.

*Proof.* (i) Let $g \in \mathbb{R}[x]_s$ with $\operatorname{vec}(g) \in \operatorname{Ker} M_s(y') \setminus \operatorname{Ker} M_s(y)$. By Claim 3.3, $g(v) = \mathbf{i}a$ for some $a \in \mathbb{R}$. As $g - af'$ vanishes at $v$ and $\overline{v}$,

$\mathrm{vec}(g) - a\,\mathrm{vec}(f') \in \mathrm{Ker}\, M_s(y)$ and thus $\mathrm{vec}(g) - a\,\mathrm{vec}(f') \in W'_0$. This shows that $\mathrm{Ker}\, M_s(y') = W'_0 + \mathbb{R}\,\mathrm{vec}(f')$.

(ii) Setting $k_0 := \dim W'_0$, we have $\dim \mathrm{Ker}\, M_s(y') = k_0 + 1$. As $W'_0 + \mathbb{R}\,\mathrm{vec}(f) \subseteq \mathrm{Ker}\, M_s(y)$, we have $\dim \mathrm{Ker}\, M_s(y) \geq k_0 + 1$; moreover equality holds for otherwise one would have $\mathrm{rank}\, M_s(y) < \mathrm{rank}\, M_s(y')$. Therefore, $\mathrm{Ker}\, M_s(y) = W'_0 + \mathbb{R}\,\mathrm{vec}(f)$.

(iii) Assume $\mathrm{vec}(g) \in W'_0$; then

$$0 = (f(\overline{v})\zeta_{s,v}\zeta_{s,v}^T + f(v)\zeta_{s,\overline{v}}\zeta_{s,\overline{v}}^T)\,\mathrm{vec}(g) f(\overline{v})g(v)\zeta_{s,v} + f(v)g(\overline{v})\zeta_{s,\overline{v}}$$

which, using Claim 3.2, implies that $f(\overline{v})g(v) = 0$ and thus $g(v) = 0$. □

CLAIM 3.5. *$f(v) = a(1+\mathbf{i})$ for some $a \in \mathbb{R}$, i.e., $\mathrm{Re}\, f(v) = \mathrm{Im}\, f(v)$.*

*Proof.* We first show that $\mathrm{vec}(f' + f'') \in \mathrm{Ker}\, M_s(y)$. Indeed,

$$\begin{gathered} -M_s(y)\,\mathrm{vec}(f' + f'') \\ = (f(\overline{v})f'(v)\zeta_{s,v} + f(v)f'(\overline{v})\zeta_{s,\overline{v}}) + \mathbf{i}(f(v)f''(\overline{v})\zeta_{s,\overline{v}} - f(\overline{v})f''(v)\zeta_{s,v}) \\ = (\mathbf{i}f(\overline{v})\zeta_{s,v} - \mathbf{i}f(v)\zeta_{s,\overline{v}}) + \mathbf{i}(f(v)\zeta_{s,\overline{v}} - f(\overline{v})\zeta_{s,v}) = 0. \end{gathered}$$

By Claim 3.4 (ii), $\mathrm{Ker}\, M_s(y) = W'_0 + \mathbb{R}\,\mathrm{vec}(f)$. Therefore, $\mathrm{vec}(f' + f'') = \mathrm{vec}(f_0) + \lambda\,\mathrm{vec}(f)$ for some $\mathrm{vec}(f_0) \in W'_0$ and $\lambda \in \mathbb{R}$. As $f_0(v) = 0$ (by Claim 3.4 (iii)), we find that $\lambda f(v) = f'(v) + f''(v) = \mathbf{i} + 1$ and thus $\mathrm{Re}\, f(v) = \mathrm{Im}\, f(v)$. □

We are now ready to conclude the proof of Theorem 3.1. We have just proven the following fact: Let $y \in \mathcal{K}_t$ for which $\mathrm{rank}\, M_s(y)$ is maximum; if $\mathrm{vec}(f) \in \mathrm{Ker}\, M_s(y)$ satisfies $f(v) \neq 0$ for some $v \in V(I) \setminus \mathbb{R}^n$, then $\mathrm{Re}\, f(v) = \mathrm{Im}\, f(v)$. On the other hand we have constructed $y' \in \mathcal{K}_t$ for which $\mathrm{rank}\, M_s(y')$ is maximum (since $\mathrm{rank}\, M_s(y') = \mathrm{rank}\, M_s(y)$ by Claim 3.4) (i) and (ii)) and $\mathrm{vec}(f') \in \mathrm{Ker}\, M_s(y')$ with $f'(v) \neq 0$ and $\mathrm{Re}\, f'(v) = 0 \neq 1 = \mathrm{Im}\, f'(v)$. Therefore we reach a contradiction. □

**3.1.3. The ingredients for our algorithm for $V_{\mathbb{C}}(I)$.** As a direct consequence of Lemma 3.1 and Theorem 3.1, if $y \in \mathcal{K}_t$ satisfies (3.3) for $D \leq s \leq \lfloor t/2 \rfloor$, then

$$I \subseteq \langle \mathrm{Ker}\, M_s(y) \rangle \subseteq I(V_{\mathbb{C}}(I)). \tag{3.4}$$

and thus $V_{\mathbb{C}}(I) = V_{\mathbb{C}}(\langle \mathrm{Ker}\, M_s(y) \rangle)$. This does not help to compute $V_{\mathbb{C}}(I)$ yet since we also need a basis of the quotient space $\mathbb{R}[x]/\langle \mathrm{Ker}\, M_s(y) \rangle$. A crucial feature is that, if moreover the matrix $M_s(y)$ is a flat extension of its submatrix $M_{s-1}(y)$ then, in view of Theorem 2.6, any basis $\mathcal{B}$ of the column space of $M_{s-1}(y)$ is a basis of the quotient space $\mathbb{R}[x]/\langle \mathrm{Ker}\, M_s(y) \rangle$. We now state the main result on which our algorithm is based.

THEOREM 3.6. *Let $y \in \mathcal{K}_t$, let $1 \leq s \leq \lfloor t/2 \rfloor$, assume that $\mathrm{rank}\, M_s(y)$ is maximum, i.e. that (3.3) holds, and consider the conditions:*

$$\mathrm{rank}\, M_s(y) = \mathrm{rank}\, M_{s-1}(y) \quad \textit{with } D \leq s \leq \lfloor t/2 \rfloor, \tag{3.5}$$

$$\mathrm{rank}\, M_s(y) = \mathrm{rank}\, M_{s-d}(y) \quad \textit{with } d \leq s \leq \lfloor t/2 \rfloor. \tag{3.6}$$

*If (3.5) or (3.6) holds then (3.4) holds and any basis of the column space of $M_{s-1}(y)$ is a basis of $\mathbb{R}[x]/\langle \operatorname{Ker} M_s(y)\rangle$. Hence one can construct the multiplication matrices in $\mathbb{R}[x]/\langle \operatorname{Ker} M_s(y)\rangle$ from the matrix $M_s(y)$ and find the variety $V_{\mathbb{C}}(\langle \operatorname{Ker} M_s(y)\rangle) = V_{\mathbb{C}}(I)$ using the eigenvalue method.*

*Proof.* Directly using Theorems 2.6, 3.1 and Lemmas 3.1, 3.2. □

The next result will be used for proving termination of our algorithm.

PROPOSITION 3.1. *Assume $1 \le |V_{\mathbb{C}}(I)| < \infty$. There exist integers $t_1, t_2$ such that, for any $t$ with $\lfloor t/2 \rfloor \ge t_1 + t_2$, $\operatorname{rank} M_{t_1}(y) = \operatorname{rank} M_{t_1-d}(y)$ holds for all $y \in \mathcal{K}_t$.*

*Proof.* Let $y \in \mathcal{K}_t$ and assume $t \ge 2D$. Then, by Lemma 3.1, $h_1, \ldots, h_m \in \operatorname{Ker} M_{\lfloor t/2 \rfloor}(y)$. We will use the following fact which follows from (3.2): For $u \in \mathbb{R}[x]$,

$$[M_{\lfloor t/2 \rfloor}(y) \operatorname{vec}(uh_j)]_\gamma = 0 \ \text{ if } |\gamma| + \deg(u) \le \lfloor t/2 \rfloor. \tag{3.7}$$

Let $\mathcal{B}$ be a basis of $\mathbb{R}[x]/I$ and set $d_{\mathcal{B}} := \max_{b \in \mathcal{B}} \deg(b)$ (which is well defined as $|\mathcal{B}| < \infty$ since $|V_{\mathbb{C}}(I)| < \infty$). Write any monomial as

$$x^\alpha = r^{(\alpha)} + \sum_{j=1}^{m} u_j^{(\alpha)} h_j,$$

where $r^{(\alpha)} \in \operatorname{Span}_{\mathbb{R}}(\mathcal{B})$ and $u_j^{(\alpha)} \in \mathbb{R}[x]$. Set $t_1 := \max(D, d_{\mathcal{B}} + d)$,

$$t_2 := \max(\deg(u_j^{(\alpha)}) \mid j = 1, \ldots, m, |\alpha| \le t_1)$$

and let $t$ be such that $\lfloor t/2 \rfloor \ge t_1 + t_2$. Let $y \in \mathcal{K}_t$; we show that $M_{t_1}(y)$ is a flat extension of $M_{t_1-d}(y)$. For this consider $\alpha, \gamma \in \mathbb{N}^n_{t_1}$. Then $|\gamma| + \deg(u_j^{(\alpha)}) \le t_1 + t_2 \le \lfloor t/2 \rfloor$. Hence, by (3.7), the $\gamma$th component of $M_{\lfloor t/2 \rfloor}(y) \operatorname{vec}(u_j^{(\alpha)} h_j)$ is equal to 0 and thus the $\gamma$th component of $M_{\lfloor t/2 \rfloor}(y) \operatorname{vec}(x^\alpha - r^{(\alpha)})$ is equal to 0. In other words, for $|\alpha| \le t_1$, the $\alpha$th column of $M_{t_1}(y)$ is a linear combination of the columns of $M_{t_1}(y)$ indexed by $\mathcal{B}$ and thus $M_{t_1}(y)$ is a flat extension of $M_{t_1-d}(y)$ as $d_{\mathcal{B}} \le t_1 - d$. □

We next provide a criterion for detecting when the variety $V_{\mathbb{C}}(I)$ is empty.

PROPOSITION 3.2. *The following statements are equivalent.*

**(i)** $V_{\mathbb{C}}(I) = \emptyset$.

**(ii)** *There exist $t_1, t_2 \in \mathbb{N}$ such that, for all $t$ with $\lfloor t/2 \rfloor \ge t_1 + t_2$ and all $y \in \mathcal{K}_t$, $y_\alpha = 0$ for all $\alpha \in \mathbb{N}^n_{t_1}$.*

*Proof.* If $v \in V_{\mathbb{C}}(I)$, then $y := \zeta_{t,v} + \zeta_{t,\bar{v}} \in \mathcal{K}_t$ with $y_0 = 2$; this showing (ii) $\Longrightarrow$ (i). Conversely, assume $V_{\mathbb{C}}(I) = \emptyset$. Then, by Hilbert's Nullstellensatz, $1 \in I$, i.e., $1 = \sum_{j=1}^m u_j h_j$ for some $u_j \in \mathbb{R}[x]$. Set $t_1 := D$,

$t_2 := \max_j \deg(u_j)$ and consider $y \in \mathcal{K}_t$ where $\lfloor t/2 \rfloor \geq t_1 + t_2$. Then, for each $j$, $[M_t(y)\,\mathrm{vec}(u_j h_j)]_\alpha = 0$ if $|\alpha| \leq t_1$ (using (3.7)). Therefore, $y_\alpha = [M_t(y)\,\mathrm{vec}(1)]_\alpha = 0$ for all $|\alpha| \leq t_1$. □

**3.1.4. Sketch of the algorithm for finding $V_{\mathbb{C}}(I)$.** We can now describe our algorithm for finding $V_{\mathbb{C}}(I)$. Algorithm 2 is similar to the one introduced in [10] for the task of computing real roots, except that now it only uses standard numerical linear algebra and *no* semidefinite programming.

**Algorithm 2** *The moment-matrix algorithm for $V_{\mathbb{C}}(I)$:*

**Input:** $t \geq D$.

**Output:** A basis $\mathcal{B} \subseteq \mathbb{R}[x]_{s-1}$ of $\mathbb{K}[x]/\langle \mathrm{Ker}\, M_s(y)\rangle$ needed to compute $V_{\mathbb{C}}(I)$.

1: Find $y \in \mathcal{K}_t$ for which $\mathrm{rank}\, M_s(y)$ is maximum for all $1 \leq s \leq \lfloor t/2 \rfloor$.
2: Check if (3.5) holds for some $D \leq s \leq \lfloor t/2 \rfloor$, or if (3.6) holds for some $d \leq s \leq \lfloor t/2 \rfloor$.
3: **if** yes **then**
4: **return** a basis $\mathcal{B} \subseteq \mathbb{R}[x]_{s-1}$ of the column space of $M_{s-1}(y)$, and extract $V_{\mathbb{C}}(I)$ (applying the eigenvalue method to the quotient space $\mathbb{R}[x]/\langle \mathrm{Ker}\, M_s(y)\rangle$ with basis $\mathcal{B}$).
5: **else**
6: Iterate (go to 1)) replacing $t$ by $t+1$
7: **end if**

REMARK 3.1. Proposition 3.1 guarantees the termination of this algorithm.

More details concerning Step 2 (in particular, about finding a basis of the column space and implementing the eigenvalue method) can be found in our preceding paper [10]. We now discuss the issue raised in Step 1 of Algorithm 2, that is, how to find $y \in \mathcal{K}_t$ satisfying

$$\forall s,\ 1 \leq s \leq \lfloor t/2 \rfloor,\ \mathrm{rank}\, M_s(y) = \max_{z \in \mathcal{K}_t} \mathrm{rank}\, M_s(z) =: R_{t,s}. \tag{3.8}$$

As we now show, this property is in fact a generic property of $\mathcal{K}_t$, i.e. the set of points $y \in \mathcal{K}_t$ that do not have this property has measure 0. For this, set $N_t := \dim \mathcal{K}_t$ and let $z_1, \ldots, z_{N_t} \in \mathbb{R}^{\mathbb{N}^n_t}$ be a linear basis of $\mathcal{K}_t$, so that $\mathcal{K}_t = \{ \sum_{i=1}^{N_t} a_i z_i \mid a_i \in \mathbb{R} \}$. For $1 \leq s \leq \lfloor t/2 \rfloor$, set

$$\Omega_{t,s} := \left\{ a = (a_1, \ldots, a_{N_t}) \in \mathbb{R}^{N_t} \mid \mathrm{rank}\, M_s\Big( \sum_{i=1}^{N_t} a_i z_i \Big) < R_{t,s} \right\}.$$

LEMMA 3.3. *$\Omega_{t,s} = V_{\mathbb{R}}(\mathcal{P}_{t,s})$ for some finite set $\mathcal{P}_{t,s} \subseteq \mathbb{R}[x_1, \ldots, x_{N_t}]$ containing at least one nonzero polynomial.*

*Proof.* The condition $\operatorname{rank} M_s(\sum_{i=1}^{N_t} a_i z_i) < R_{t,s}$ is equivalent to requiring that all $R_{t,s} \times R_{t,s}$ submatrices of $M_s(\sum_{i=1}^{N_t} a_i z_i)$ have zero determinant. Each such determinant can be expressed as a polynomial in the variables $a_1, \ldots, a_{N_t}$. Therefore there exists a finite set $\mathcal{P}_{t,s}$ of polynomials in $\mathbb{R}[x_1, \ldots, x_{N_t}]$ for which $\Omega_{t,s} = V_{\mathbb{R}}(\mathcal{P}_{t,s})$. By definition of $R_{t,s}$, there exists $a \in \mathbb{R}^{N_t}$ for which $\operatorname{rank} M_s(\sum_i a_i z_i) = R_{t,s}$. Hence, at least one $R_{t,s} \times R_{t,s}$ minor of $M_s(\sum_i a_i z_i)$ is nonzero; that is, $p(a) \neq 0$ for some $p \in \mathcal{P}_{t,s}$ and so $p$ is nonzero. □

Note that $\{a \in \mathbb{R}^{N_t} \mid \exists s \leq \lfloor t/2 \rfloor \text{ with } \operatorname{rank} M_s(\sum_i a_i z_i) < R_{t,s}\} = \bigcup_{s=1}^{\lfloor t/2 \rfloor} \Omega_{t,s}$; by Lemma 3.3, this set has Lebesgue measure 0, which shows that the property (3.8) is a generic property of the set $\mathcal{K}_t$. This shows:

COROLLARY 3.1. *The subset $G_t \subseteq \mathcal{K}_t$ of all generic elements (i.e. satisfying (3.8)) of $\mathcal{K}_t$ is dense in $\mathcal{K}_t$.*

Our strategy for Step 1 of Algorithm 2 is to choose $y = \sum_{i=1}^{N_t} a_i z_i$ where the scalars $a_i$ are picked randomly according to e.g. a uniform probability distribution on $[0, 1]$. Then the maximality property (3.8) holds almost surely for $y$.

EXAMPLE 1. The following example

$$\begin{aligned} h_1 &= x_1^2 - 2x_1x_3 + 5\,, \\ h_2 &= x_1x_2^2 + x_2x_3 + 1\,, \\ h_3 &= 3x_2^2 - 8x_1x_3\,, \end{aligned}$$

taken from [4, Ex. 4, p.57], is used to illustrate Algorithm 2. Table 1 shows the ranks of the matrices $M_s(y)$ for generic $y \in \mathcal{K}_t$, as a function of $s$ and $t$. Condition (3.5) is satisfied e.g. for $t = 8$ and $s = 3$ as we have:

$$\operatorname{rank} M_3(y) = \operatorname{rank} M_2(y), \text{ with } y \in \mathcal{K}_8.$$

TABLE 1
*Rank of $M_s(y)$ for generic $y \in \mathcal{K}_t$ in Example 1.*

| | $t=2$ | $t=4$ | $t=6$ | $t=8$ |
|---|---|---|---|---|
| $s=0$ | 1 | 1 | 1 | 1 |
| $s=1$ | 4 | 4 | 4 | 4 |
| $s=2$ | | 8 | 8 | **8** |
| $s=3$ | | | 9 | **8** |
| $s=4$ | | | | 9 |

Applying Algorithm 2 we have computed the following 8 complex solutions:

$$
\begin{aligned}
v_1 &= \left[\ -1.101, -2.878, -2.821\ \right],\\
v_2 &= \left[\ 0.07665 + 2.243i, 0.461 + 0.497i, 0.0764 + 0.00834i\ \right],\\
v_3 &= \left[\ 0.07665 - 2.243i, 0.461 - 0.497i, 0.0764 - 0.00834i\ \right],\\
v_4 &= \left[\ -0.081502 - 0.93107i, 2.350 + 0.0431i, -0.274 + 2.199i\ \right],\\
v_5 &= \left[\ -0.081502 + 0.93107i, 2.350 - 0.0431i, -0.274 - 2.199i\ \right],\\
v_6 &= \left[\ 0.0725 + 2.237i, -0.466 - 0.464i, 0.0724 + 0.00210i\ \right],\\
v_7 &= \left[\ 0.0725 - 2.237i, -0.466 + 0.464i, 0.0724 - 0.00210i\ \right],\\
v_8 &= \left[\ 0.966, -2.813, 3.072\ \right]
\end{aligned}
$$

with maximum error of $\epsilon := \max_{i\le 8, j\le 3} |h_j(v_i)| \le 3 \cdot 10^{-10}$. For the sake of comparison, Table 2 displays the ranks of the matrices $M_s(y)$ for generic $y \in \mathcal{K}_{t,\succeq}$; now the rank condition (3.5) is satisfied at $s = 2$ and $t = 6$; that is,

$$\operatorname{rank} M_2(y) = \operatorname{rank} M_1(y), \text{ with } y \in \mathcal{K}_{6,\succeq}.$$

TABLE 2
*Rank of $M_s(y)$ for generic $y \in \mathcal{K}_{t,\succeq}$ in Example 1.*

| | $t=2$ | $t=4$ | $t=6$ |
|---|---|---|---|
| $s=0$ | 1 | 1 | 1 |
| $s=1$ | 4 | 4 | **2** |
| $s=2$ | | 8 | **2** |
| $s=3$ | | | 3 |

The real roots extracted with the algorithm proposed in [10] are

$$
\begin{aligned}
v_1 &= \left[\ -1.101, -2.878, -2.821\ \right],\\
v_2 &= \left[\ 0.966, -2.813, 3.072\ \right],
\end{aligned}
$$

with a maximum error of $\epsilon \le 9 \cdot 10^{-11}$.

**3.2. The Gorenstein case.** We address here the question of when equality $I = \langle \operatorname{Ker} M_s(y)\rangle$ can be attained in (3.4). We begin with an example showing that both inclusions in (3.4) may be strict.

EXAMPLE 2. Consider the ideal $I = \langle x_1^2, x_2^2, x_1x_2\rangle \subseteq \mathbb{R}[x_1, x_2]$. Then, $V_{\mathbb{C}}(I) = \{0\}$, $I(V_{\mathbb{C}}(I)) = \langle x_1, x_2\rangle$, $\dim \mathbb{R}[x]/I = 3$ (with basis $\{1, x_1, x_2\}$), and $\dim \mathbb{R}[x]/I(V_{\mathbb{C}}(I)) = 1$ (with basis $\{1\}$). On the other hand, we have $\dim \mathbb{R}[x]/\langle \operatorname{Ker} M_s(y)\rangle = 2$ (with base $\{1, x_1\}$ or $\{1, x_2\}$) for any generic $y \in \mathcal{K}_t$ (i.e. satisfying the maximality property (3.8)) and $t \ge 2$, $1 \le s \le \lfloor t/2\rfloor$. Indeed any such $y$ satisfies $y_\alpha = 0$ for all $|\alpha| \ge 2$; therefore its moment matrix has the form

$$M_{\lfloor t/2 \rfloor}(y) = \begin{pmatrix} y_{00} & y_{10} & y_{01} & 0\dots \\ y_{10} & 0 & 0 & 0\dots \\ y_{01} & 0 & 0 & 0\dots \\ 0 & 0 & 0 & 0\dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

(indexing $M_{\lfloor t/2 \rfloor}(y)$ by $1, x_1, x_2, x_1^2, x_1x_2, x_2^2, \dots$), with

$$L_y = y_{00}\partial_{00}[0] + y_{10}\partial_{10}[0] + y_{01}\partial_{01}[0]\,.$$

Hence, $R_{t,0} = 1$ and for $s \geq 1$ $R_{t,s} = 2$ where, for generic $y_1, y_2 \in \mathcal{K}_t$, e.g. $\langle \operatorname{Ker} M_s(y_1)\rangle = \langle x_1, x_1x_2, x_2^2\rangle$ or $\langle \operatorname{Ker} M_s(y_2)\rangle = \langle x_2, x_1x_2, x_1^2\rangle$ is a strict superset of $I$ and a strict subset of $I(V_{\mathbb{C}}(I))$.

Following Cox [6, Chapter 2], call an algebra $\mathcal{A}$ *Gorenstein* if there exists a nongenerate bilinear form

$$(\cdot,\cdot) : \mathcal{A} \times \mathcal{A} \to \mathbb{R}$$

satisfying $(fg, h) = (f, gh)$ for all $f, g, h \in \mathcal{A}$ (equivalently, if $\mathcal{A}$ and its dual space are isomorphic $\mathcal{A}$-modules). Consider the quotient algebra $\mathcal{A} = \mathbb{R}[x]/I$ where $I = \langle h_1, \dots, h_m\rangle$ is an ideal in $\mathbb{R}[x]$. Then any bilinear form on $\mathbb{R}[x]/I \times \mathbb{R}[x]/I$ is of the form

$$(f, g) \quad \mapsto \quad (f, g)_y := \operatorname{vec}(f)^T M(y) \operatorname{vec}(g)$$

for some $y \in \mathcal{K}_\infty$, after setting

$$\mathcal{K}_\infty := \{y \in \mathbb{R}^{\mathbb{N}^n} \mid I \subseteq \operatorname{Ker} M(y)\}.$$

Moreover the bilinear form $(\cdot,\cdot)_y$ is nondegenerate precisely when $I = \operatorname{Ker} M(y)$. As $I = \operatorname{Span}_{\mathbb{R}}(\cup_{t\geq 1}\mathcal{H}_t)$, we have

$$\mathcal{K}_\infty = \{y \in \mathbb{R}^{\mathbb{N}^n} \mid L_y(p) = y^T \operatorname{vec}(p) = 0 \ \forall p \in \cup_{t\geq 1}\mathcal{H}_t\}.$$

That is, $\mathcal{K}_\infty$ is the analogue of the sets $\mathcal{K}_t$ for $t = \infty$, and $\mathcal{K}_\infty$ is isomorphic to the dual space $\mathcal{D}[I] = I^\perp$ (recall (2.2)). Based on the above observations and Theorem 2.6 we obtain:

PROPOSITION 3.3. *Let $I = \langle h_1, \dots, h_m\rangle$ be a zero-dimensional ideal in $\mathbb{R}[x]$. The following assertions are equivalent.*

**(i)** *The algebra $\mathbb{R}[x]/I$ is Gorenstein.*

**(ii)** *There exists $y \in \mathbb{R}^{\mathbb{N}^n}$ such that $I = \operatorname{Ker} M(y)$.*

**(iii)** *There exist $t \geq 1$ and $y \in \mathcal{K}_{2t}$ such that $\operatorname{rank} M_t(y) = \operatorname{rank} M_{t-1}(y)$ and $I = \langle \operatorname{Ker} M_t(y)\rangle$.*

*Proof.* The equivalence of (i), (ii) follows from the definition of a Gorenstein algebra and the above observations. Assume (ii) holds. Let $\mathcal{B}$ be a basis of $\mathbb{R}[x]/I$ and suppose $\mathcal{B} \subseteq \mathbb{T}^n_{t-1}$. It is immediate to verify

that $\mathcal{B}$ indexes a maximal linearly independent set of columns of $M(y)$. Hence, $\operatorname{rank} M_{t-1}(y) = \operatorname{rank} M(y) = \operatorname{rank} M_t(y)$ and $I = \langle \operatorname{Ker} M_t(y) \rangle$ (by Theorem 2.6). Thus (iii) holds. The reverse implication (iii) $\Longrightarrow$ (ii) follows directly from Theorem 2.6. □

EXAMPLE 3. Consider the ideal $I = \langle x_1^2, x_2^2 \rangle \subseteq \mathbb{R}[x_1, x_2]$. Then $\dim \mathbb{R}[x]/I = 4$ and for $y \in \mathcal{K}_{2t}$ $(t \geq 2)$,

$$M_t(y) = \begin{pmatrix} y_{00} & y_{10} & y_{01} & y_{11} & 0 \dots \\ y_{10} & 0 & y_{11} & 0 & 0 \dots \\ y_{01} & y_{11} & 0 & 0 & 0 \dots \\ y_{11} & 0 & 0 & 0 & 0 \dots \\ 0 & 0 & 0 & 0 & 0 \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Hence the maximal rank of $M_t(y)$ is equal to 4 and for any such $y$, $I = \langle \operatorname{Ker} M_t(y) \rangle$. Thus $\mathbb{R}[x]/I$ is Gorenstein. Similarly, $\mathbb{R}[x]/I$ is also Gorenstein when $I = \langle x_1, x_2^3 \rangle$, but not for the ideal $I$ of Example 2.

The next lemma illustrates how the kernels of moment matrices $M_t(y)$ for $y \in K_t$ are related to the ideal $I$ even in the non-Gorenstein case.

LEMMA 3.4. *Assume that the ideal $I$ is zero-dimensional. Then,*

**(i)** *Let $\{w_1, \dots, w_N\}$ be a linear basis of $\mathcal{K}_\infty$. Then*

$$I = \bigcap_{i=1}^{N} \langle \operatorname{Ker} M(w_i) \rangle.$$

**(ii)** *Let $z_1, \dots, z_{N_t}$ be a basis of $\mathcal{K}_t$. Then*

$$\Big\langle \bigcap_{i=1}^{N_t} \operatorname{Ker} M_{\lfloor t/2 \rfloor}(z_i) \Big\rangle \subseteq I,$$

*with equality for $\lfloor t/2 \rfloor \geq D$.*

*Proof.* (i) The inclusion $I \subseteq \cap_{i=1}^N \operatorname{Ker} M(w_i)$ is obvious. Conversely, let $q \in \mathbb{R}[x]$ with $\operatorname{vec}(q) \in \cap_{i=1}^N \operatorname{Ker} M(w_i)$; we show that $q \in I$ or, equivalently, that $L(q) = 0$ for all $L \in (\mathbb{R}[x]/I)^*$. Let $L \in (\mathbb{R}[x]/I)^*$ and so $L = L_y$ for some $y = \sum_{i=1}^N a_i w_i$ with $a_i \in \mathbb{R}$. Hence $L(q) = \sum_i a_i w_i^T \operatorname{vec}(q) = 0$ since $w_i^T \operatorname{vec}(q) = 1^T M(w_i) \operatorname{vec}(q) = 0$.
(ii) Let $q \in \mathbb{R}[x]$ with $\operatorname{vec}(q) \in \cap_{i=1}^{N_t} \operatorname{Ker} M_{\lfloor t/2 \rfloor}(z_i)$; we show that $q \in I$. Again it suffices to show that $L(q) = 0$ for every $L \in (\mathbb{R}[x]/I)^*$. As above let $L = L_y$ with $y = \sum_{i=1}^N a_i w_i$. As $w_i \in \mathcal{K}_\infty$, its projection $\pi_t(w_i)$ is an element of $\mathcal{K}_t$ and thus is of the form $\sum_{j=1}^{N_t} \lambda_{i,j} z_j$ for some scalars $\lambda_{i,j}$. Hence $L(q) = L_y(q) = \sum_i a_i \sum_j \lambda_{i,j} z_j^T \operatorname{vec}(q) = 0$ since $z_j^T \operatorname{vec}(q) = 0 \; \forall \, j = 1, \dots, N_t$. If $\lfloor t/2 \rfloor \geq D$ then $\operatorname{vec}(h_j) \in \operatorname{Ker} M_{\lfloor t/2 \rfloor}(y)$ for all $y \in \mathcal{K}_t$ using Lemma 3.1, which gives the desired equality $I = \langle \cap_{i=1}^{N_t} \operatorname{Ker} M_{\lfloor t/2 \rfloor}(z_i) \rangle$. □

**4. Link with other symbolic-numeric methods.** In this section we explore the links between the moment based approach from the preceding section with other methods in the literature, in particular the work of Zhi and Reid [18] and Mourrain et al. [15, 17]. The method we discuss here again uses the sets $\mathcal{K}_t$ introduced in (1.2) but is more global. Namely while in the moment based method we used a generic point $y \in \mathcal{K}_t$, we now use the full set $\mathcal{K}_t$ and its defining equations. More precisely, while in the moment based method the stopping criterion was a certain rank condition ((3.5) or (3.6)) on moment matrices $M_s(y)$ for a generic point $y \in \mathcal{K}_t$, the stopping criterion is now formulated in terms of the dimension of projections $\pi_s(\mathcal{K}_t)$ of the set $\mathcal{K}_t$.

The basic techniques behind the work [18] originally stem from the treatment of partial differential equations. Zharkov et al. [25, 26] were the first to apply these techniques to polynomial ideals. We will describe the idea of their algorithm (a simplified version, based on [18]) for the complex case in Section 4.1, using the language (rewriting families, multiplication matrices, etc.) presented earlier in the paper. Then, in Section 4.2 we show relations between the stopping criteria for the moment based method and the Zhi-Reid method. In a follow-up work [9] we will show that the method can be extended to the computation of real roots by adding some positivity constraints, thus working with the set $\mathcal{K}_{t,\succeq}$ in place of $\mathcal{K}_t$.

**4.1. Dual space characterization of $I$.** Again consider the sets $\mathcal{H}_t$ and $\mathcal{K}_t$ in (1.1) and (1.2). $\mathcal{K}_t$ is a linear subspace of $(\mathbb{R}[x]_t)^*$ and $\mathcal{K}_t^\perp = \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_t)$. For $s \le t$, recall that $\pi_s$ is the projection from $(\mathbb{R}[x]_t)^*$ onto $(\mathbb{R}[x]_s)^*$. Note that

$$(\pi_s(\mathcal{K}_t))^\perp = \mathcal{K}_t^\perp \cap \mathbb{R}[x]_s = \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_t) \cap \mathbb{R}[x]_s. \tag{4.1}$$

Recall that $\mathcal{D}[I] = I^\perp = \{L \in (\mathbb{R}[x])^* \mid L(p) = 0 \ \forall p \in I\}$ is isomorphic to the set $\mathcal{K}_\infty$ (by the linear mapping $y \mapsto L_y$). As $\mathcal{H}_t \subseteq I$, we have

$$\pi_s(\mathcal{D}[I]) \subseteq \pi_s(\mathcal{K}_t),\ \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_t) \cap \mathbb{R}[x]_s = (\pi_s(\mathcal{K}_t))^\perp \subseteq I \cap \mathbb{R}[x]_s. \tag{4.2}$$

We will show some dimension conditions on $\mathcal{K}_t$ ensuring that equality holds in (4.2), thus leading to a dual space characterization of $I$. The main result of this section is the following theorem, similar to some well known results from the theory of involutive bases (see [21]) and used e.g. in the algorithm of [18].

THEOREM 4.1. *Let $I = \langle h_1, \ldots, h_m \rangle$ be an ideal in $\mathbb{R}[x]$ and $D = \max_j \deg(h_j)$. Consider the following two conditions*

$$\dim \pi_s(\mathcal{K}_t) = \dim \pi_{s-1}(\mathcal{K}_t), \tag{4.3a}$$

$$\dim \pi_s(\mathcal{K}_t) = \dim \pi_s(\mathcal{K}_{t+1}). \tag{4.3b}$$

*Assume that (4.3a) and (4.3b) hold for some integer $s$ with $D \le s \le t$. If $\dim \pi_{s-1}(\mathcal{K}_t) = 0$ then $V_{\mathbb{C}}(I) = \emptyset$. Otherwise let $\mathcal{B} \subseteq \mathbb{T}^n_{s-1}$ satisfying*

$$\pi_{s-1}(\mathcal{K}_t) \oplus \mathrm{Span}_{\mathbb{R}}(\{\partial_\alpha[0] \mid x^\alpha \in \mathbb{T}^n_{s-1} \setminus \mathcal{B}\}) = (\mathbb{R}[x]_{s-1})^*$$

*and assume that $\mathcal{B}$ is connected to 1.*[1] *Then,*

- *$\mathcal{B}$ is a basis of $\mathbb{R}[x]/I$*
- *$\pi_s(\mathcal{D}[I]) = \pi_s(\mathcal{K}_t)$ and $I \cap \mathbb{R}[x]_s = \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_t) \cap \mathbb{R}[x]_s$, i.e. equality holds in (4.2).*

*Proof.* Set $N := \dim \pi_{s-1}(\mathcal{K}_t)$. If $N = 0$, then $\pi_{s-1}(\mathcal{K}_t) = \{0\}$, $(\pi_{s-1}(\mathcal{K}_t))^\perp = \mathbb{R}[x]_{s-1}$ implying $1 \in I$ and thus $V_{\mathbb{C}}(I) = \emptyset$. Assume now $N \geq 1$. Let $\{L_1, \ldots, L_N\} \subseteq \mathcal{K}_t$ such that $\mathcal{L}_1 := \{\pi_{s-1}(L_j) \mid j = 1, \ldots, N\}$ forms a basis of $\pi_{s-1}(\mathcal{K}_t)$. We can complete $\mathcal{L}_1$ to a basis of $(\mathbb{R}[x]_{s-1})^*$ using members of the canonical basis. That is, let $\mathcal{B} \subseteq \mathbb{T}^n_{s-1}$, $|\mathcal{B}| = N$, $\mathcal{L}_2 := \{\partial_\alpha[0] \mid x^\alpha \in \mathbb{T}^n_{s-1} \setminus \mathcal{B}\}$ such that $\mathcal{L}_1 \cup \mathcal{L}_2$ is a basis of $(\mathbb{R}[x]_{s-1})^*$. We claim that

$$(\pi_{s-1}(\mathcal{K}_t)^\perp \oplus \mathrm{Span}_{\mathbb{R}}(\mathcal{B}) = \mathbb{R}[x]_{s-1}. \tag{4.4}$$

It suffices to verify that $\mathrm{Span}_{\mathbb{R}}(\mathcal{B}) \cap (\pi_{s-1}(\mathcal{K}_t))^\perp = \{0\}$ as the dimensions of both sides then coincide. Indeed, if $p \in \mathrm{Span}_{\mathbb{R}}(\mathcal{B})$, then $L(p) = 0$ if $L = \partial_\alpha[0]$ ($x^\alpha \in \mathbb{T}^n_{s-1} \setminus \mathcal{B}$) since $p$ uses only monomials from $\mathcal{B}$, and if $p \in (\pi_{s-1}(\mathcal{K}_t))^\perp$ then $L(p) = 0$ if $L = L_j$ ($j \leq N$).

As the set $\{\pi_s(L_j) \mid j \leq N\}$ is linearly independent in $\pi_s(\mathcal{K}_t)$ and $N = \dim \pi_s(\mathcal{K}_t)$ by (4.3*a*), this set is in fact a basis of $\pi_s(\mathcal{K}_t)$ and the analogue of (4.4) holds:

$$(\pi_s(\mathcal{K}_t))^\perp \oplus \mathrm{Span}_{\mathbb{R}}(\mathcal{B}) = \mathbb{R}[x]_s. \tag{4.5}$$

In particular, $\mathrm{Span}_{\mathbb{R}}(\mathcal{B}) \cap (\pi_s(\mathcal{K}_t))^\perp = \{0\}$ and any polynomial $p \in \mathbb{R}[x]_s$ can be written in a unique way as $p = r_p + f_p$, where $r_p \in \mathrm{Span}_{\mathbb{R}}(\mathcal{B})$ and $f_p \in (\pi_s(\mathcal{K}_t))^\perp = \mathbb{R}[x]_s \cap \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_t)$. Thus $f_p = 0$ if $p \in \mathrm{Span}_{\mathbb{R}}(\mathcal{B})$. Set

$$F_0 := \{f_m \mid m \in \partial\mathcal{B}\} \subseteq F := \{f_m \mid m \in \mathbb{T}^n_s\} \subseteq \mathbb{R}[x]_s \cap \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_t) \subseteq I. \tag{4.6}$$

Thus $F_0$ is a rewriting family for $\mathcal{B}$ and $F \subseteq \mathbb{R}[x]_s \cap \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_t) \subseteq \mathbb{R}[x]_s \cap I$.

LEMMA 4.1. *$\mathrm{Span}_{\mathbb{R}}(F) = \mathbb{R}[x]_s \cap \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_t)$. In particular, $I = \langle F \rangle$ if $s \geq D = \max_j \deg(h_j)$.*

*Proof.* Let $p \in (\pi_s(\mathcal{K}_t))^\perp = \mathbb{R}[x]_s \cap \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_t)$. Write

$$p = \sum_{m \in \mathbb{T}^n_s} \lambda_m m = \sum_{m \in \mathbb{T}^n_s} \lambda_m (r_m + f_m) = r + f,$$

where $r := \sum_{m \in \mathbb{T}^n_s} \lambda_m r_m \in \mathrm{Span}_{\mathbb{R}}(\mathcal{B})$ and $f := \sum_{m \in \mathbb{T}^n_s} \lambda_m f_m \in \mathrm{Span}_{\mathbb{R}}(F)$. Thus $p - f = r \in \mathrm{Span}_{\mathbb{R}}(\mathcal{B}) \cap (\pi_s(\mathcal{K}_t))^\perp = \{0\}$, showing $p = f \in \mathrm{Span}_{\mathbb{R}}(F)$. If $s \geq D$, then each $h_j$ lies in $\mathbb{R}[x]_s \cap \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_t)$, equal to $\mathrm{Span}_{\mathbb{R}}(F)$ by the above; this thus gives $I = \langle F \rangle$. □

As $\pi_s(\mathcal{K}_{t+1}) \subseteq \pi_s(\mathcal{K}_t)$, condition (4.3*b*) implies equality of these two sets and thus of their orthogonal complements, i.e. $\mathbb{R}[x]_s \cap \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_t) =$

[1] That such a basis connected to 1 exists is proved in [9].

$\mathbb{R}[x]_s \cap \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_{t+1})$ (recall (4.1)). The next lemma shows that $(\pi_s(\mathcal{K}_t))^\perp = \mathbb{R}[x]_s \cap \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_t)$ enjoys some ideal like properties.

LEMMA 4.2. *If $f \in (\pi_s(\mathcal{K}_t))^\perp$ and $\deg(fg) \le s$ then $fg \in (\pi_s(\mathcal{K}_t))^\perp$.*

*Proof.* It is sufficient to show the result for $g = x_i$. If $f \in (\pi_s(\mathcal{K}_t))^\perp = \mathbb{R}[x]_s \cap \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_t)$, then $x_i f \in \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_{t+1})$. As $\deg(x_i f) \le s$, $x_i f \in \mathbb{R}[x]_s \cap \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_{t+1}) = \mathbb{R}[x]_s \cap \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_t)$ by (4.3*b*). ∎

Note that $1 \notin (\pi_s(\mathcal{K}_t))^\perp$; otherwise we would have $(\pi_s(\mathcal{K}_t))^\perp = \mathbb{R}[x]_{s-1}$ (by Lemma 4.2) and thus $\mathrm{Span}_{\mathbb{R}}(\mathcal{B}) = \{0\}$ (by (4.5)), contradicting our assumption $N \ge 1$. Hence we can choose the basis $\mathcal{B}$ satisfying (4.5) in such a way that $1 \in \mathcal{B}$. We now establish a relation between the two families $F$ and $F_0$.

LEMMA 4.3. *If $1 \in \mathcal{B}$ then $F \subseteq \langle F_0 \rangle$ and so $\langle F \rangle = \langle F_0 \rangle$.*

*Proof.* Consider $m \in \mathbb{T}_s \setminus \mathcal{B}^+$. Write $m = x_i m_1$. Then,

$$f_m = m - r_m = x_i m_1 - r_m = x_i(r_{m_1} + f_{m_1}) - r_m = x_i r_{m_1} + x_i f_{m_1} - r_m.$$

We have $x_i r_{m_1} = r_{x_i r_{m_1}} + f_{x_i r_{m_1}}$, where $r_{x_i r_{m_1}} \in \mathrm{Span}_{\mathbb{R}}(\mathcal{B})$ and $f_{x_i r_{m_1}} \in \mathrm{Span}_{\mathbb{R}}(F_0)$ since $x_i r_{m_1} \in \mathrm{Span}_{\mathbb{R}}(\mathcal{B}^+)$. Moreover, $f_m \in F \subseteq \pi_s(\mathcal{K}_t))^\perp$, $r := r_{x_i r_{m_1}} - r_m \in \mathrm{Span}_{\mathbb{R}}(\mathcal{B})$, and $x_i f_{m_1} \in (\pi_s(\mathcal{K}_t))^\perp$ (by Lemma 4.2 since $f_{m_1} \in (\pi_s(\mathcal{K}_t))^\perp$). Therefore, $f_m - f_{x_i r_{m_1}} - x_i f_{m_1} = r \in \mathrm{Span}_{\mathbb{R}}(\mathcal{B}) \cap (\pi_s(\mathcal{K}_t))^\perp$ is thus equal to 0. This shows $f_m = f_{x_i r_{m_1}} + x_i f_{m_1}$, where $f_{x_i r_{m_1}} \in \mathrm{Span}_{\mathbb{R}}(F_0)$. Using induction on the distance of $m$ to $\mathcal{B}$, we can conclude that $f_m \in \langle F_0 \rangle$. (The distance of $m$ to $\mathcal{B}$ is defined as the minimum value of $|\alpha|$ for which $m = x^\alpha x^\beta$ with $x_\beta \in \mathcal{B}$; it is at most $\deg(m)$ since $1 \in \mathcal{B}$.) ∎

Using the rewriting family $F_0$ we can construct the formal multiplication matrices $\mathcal{X}_1, \ldots, \mathcal{X}_n$. Next we show that they commute pairwise.

LEMMA 4.4. *The formal multiplication matrices $\mathcal{X}_i$ defined using the rewriting family $F_0$ commute pairwise.*

*Proof.* Recall that the formal multiplication operator $\mathcal{X}_i$ is defined by $\mathcal{X}_i(m) = x_i m - f_{x_i m} = r_{x_i m}$ for any $m \in \mathcal{B}$ (and extended by linearity to $\mathrm{Span}_{\mathbb{R}}(\mathcal{B})$). We have to show that $\mathcal{X}_i(\mathcal{X}_j(m_0)) = \mathcal{X}_j(\mathcal{X}_i(m_0))$ for all $i, j \le n$ and $m_0 \in \mathcal{B}$. Let $m_0 \in \mathcal{B}$. Assume first that $x_i m_0, x_j m_0 \notin \mathcal{B}$ and thus lie in $\partial\mathcal{B}$. We have: $\mathcal{X}_i(m_0) = r_{x_i m_0} := \sum_{b \in \mathcal{B}} a_b^i b$, implying $\mathcal{X}_j(\mathcal{X}_i(m_0)) = \mathcal{X}_j(\sum_{b \in \mathcal{B}} a_b^i b) = \sum_{b \in \mathcal{B}} a_b^i \mathcal{X}_j(b) = \sum_{b \in \mathcal{B}} a_b^i (x_j b - f_{x_j b}) = x_j(x_i m_0 - f_{x_i m_0}) - \sum_{b \in \mathcal{B}} a_b^i f_{x_j b}$. Analogously, $\mathcal{X}_i(\mathcal{X}_j(m_0)) = x_i(x_j m_0 - f_{x_j m_0}) - \sum_{b \in \mathcal{B}} a_b^j f_{x_i b}$. Therefore,

$$\begin{aligned} p :&= \mathcal{X}_j(\mathcal{X}_i(m_0)) - \mathcal{X}_i(\mathcal{X}_j(m_0)) \\ &= \underbrace{x_i f_{x_j m_0} - x_j f_{x_i m_0}}_{q_1} + \underbrace{\sum_{b \in \mathcal{B}} a_b^j f_{x_i b} - \sum_{b \in \mathcal{B}} a_b^i f_{x_j b}}_{q_2}. \end{aligned}$$

Now, $\deg(p) \leq s$ (as $p \in \mathrm{Span}_{\mathbb{R}}(\mathcal{B})$), $\deg(q_2) \leq s$, implies $\deg(q_1) \leq s$. Moreover, $q_1 \in (\pi_s(\mathcal{K}_t))^\perp$ (by Lemma 4.2) and $q_2 \in \mathrm{Span}_{\mathbb{R}}(F)(\pi_s(\mathcal{K}_t))^\perp$ (by Lemma 4.1). Therefore, $p \in \mathrm{Span}_{\mathbb{R}}(\mathcal{B}) \cap (\pi_s(\mathcal{K}_t))^\perp = \{0\}$, which shows the desired identity $\mathcal{X}_i(\mathcal{X}_j(m_0)) = \mathcal{X}_j(\mathcal{X}_i(m_0))$. The proof is analogous in the other cases; say, $x_i m_0 \in \mathcal{B}$, $x_j m_0 \in \partial\mathcal{B}$. ∎

COROLLARY 4.1. *Assume $\mathcal{B}$ is connected to 1. Then,*
- *$\mathcal{B}$ is a basis of $\mathbb{R}[x]/\langle F_0\rangle = \mathbb{R}[x]/\langle F\rangle = \mathbb{R}[x]/I$.*
- *$(\pi_s(\mathcal{K}_t))^\perp = \mathbb{R}[x]_s \cap \mathrm{Span}_{\mathbb{R}}(\mathcal{H}_t)$ and $\pi_s(\mathcal{K}_t) = \pi_s(\mathcal{D}[I])$.*

*Proof.* As $\mathcal{B}$ is connected to 1, $F_0$ is a rewriting family for $\mathcal{B}$, and the associated multiplication matrices commute pairwise (by Lemma 4.4), we can conclude using Theorem 2.4 that the set $\mathcal{B}$ is a basis of $\mathbb{R}[x]/\langle F_0\rangle$. Now $\langle F_0\rangle = \langle F\rangle$ (by Lemma 4.3) and $I = \langle F\rangle$ since $s \geq D$ (by Lemma 4.1). Finally, write $p \in I \cap \mathbb{R}[x]_s$ as $p = r + q$, where $r \in \mathrm{Span}_{\mathbb{R}}(\mathcal{B})$ and $q \in (\pi_s(\mathcal{K}_t))^\perp \subseteq I$ (by (4.1)). Thus $p - q = r \in \mathrm{Span}_{\mathbb{R}}(\mathcal{B}) \cap I = \{0\}$, which shows the identity $I \cap \mathbb{R}[x]_s = (\pi_s(\mathcal{K}_t))^\perp$ and thus $\pi_s(\mathcal{D}[I]) = \pi_s(\mathcal{K}_t)$. ∎

This concludes the proof of Theorem 4.1. ∎

EXAMPLE 4. We continue with Example 1 to illustrate the condition on the dimension of $\mathcal{K}_t$ and its projections $\pi_s(\mathcal{K}_t)$. Table 3 shows the dimension of the set $\pi_s(\mathcal{K}_t)$ for various orders $t$ and projection orders $s$. Note that the conditions (4.3$a$) and (4.3$b$) are satisfied at $(t, s) = (7, 4)$, i.e.

$$\dim \pi_4(\mathcal{K}_7) = \dim \pi_3(\mathcal{K}_7)$$
$$\dim \pi_4(\mathcal{K}_7) = \dim \pi_4(\mathcal{K}_8)\,.$$

TABLE 3
*Dimension of the set $\pi_s(\mathcal{K}_t)$ in Example 4.*

| | $t=3$ | $t=4$ | $t=5$ | $t=6$ | $t=7$ | $t=8$ | $t=9$ |
|---|---|---|---|---|---|---|---|
| $s=0$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $s=1$ | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| $s=2$ | 7 | 7 | 7 | 7 | 7 | 7 | 7 |
| $s=3$ | 11 | 10 | 9 | 8 | **8** | 8 | 8 |
| $s=4$ | | 12 | 10 | 9 | **8** | **8** | 8 |
| $s=5$ | | | 12 | 10 | 9 | 8 | 8 |
| $s=6$ | | | | 12 | 10 | 9 | 8 |
| $s=7$ | | | | | 12 | 10 | 9 |
| $s=8$ | | | | | | 12 | 10 |
| $s=9$ | | | | | | | 12 |

**4.2. Links between the stopping criteria of both methods.** We show some connections between the stopping criteria (3.5) and (3.6) for the

moment based method and the stopping criteria (4.3*a*), (4.3*b*) for the Zhi-Reid method [18].

First we show that the rank condition (3.5) for a generic element $y \in \mathcal{K}_t$ at a pair $(t, s)$ implies the conditions (4.3*a*) – (4.3*b*) at the pair $(t, 2s)$.

PROPOSITION 4.1. *Assume* $\operatorname{rank} M_s(y) = \operatorname{rank} M_{s-1}(y)$ *for some generic* $y \in \mathcal{K}_t$ *and* $D \leq s \leq \lfloor t/2 \rfloor$. *Then,* $\dim \pi_{2s}(\mathcal{K}_t) = \dim \pi_{2s-1}(\mathcal{K}_t) = \dim \pi_{2s}(\mathcal{K}_{t+1})$, *i.e. (4.3a) and (4.3b) hold at the pair* $(t, 2s)$.

*Proof.* Consider the linear mapping

$$\begin{aligned} \varphi: \quad & \pi_{2s}(\mathcal{K}_t) \to \pi_{2s-1}(\mathcal{K}_t) \\ & \pi_{2s}(z) \mapsto \pi_{2s-1}(z). \end{aligned}$$

As $\varphi$ is onto, if we can show that $\varphi$ is one-to-one, then this will imply $\dim \pi_{2s}(\mathcal{K}_t) = \dim \pi_{2s-1}(\mathcal{K}_t)$. Let $z \in \mathcal{K}_t$ for which $\pi_{2s-1}(z) = 0$; we show that $\pi_{2s}(z) = 0$. Set $R := \operatorname{rank} M_s(y) = \operatorname{rank} M_{s-1}(y)$ and let $\mathcal{B} \subseteq \mathbb{T}^n_{s-1}$ index a maximum linearly independent set of columns of $M_{s-1}(y)$, thus also of $M_s(y)$. Consider the element $y' := y + z$. Thus $\pi_{2s-1}(y') = \pi_{2s-1}(y)$ and the matrices $M_s(y)$ and $M_s(y')$ differ only at their entries indexed by $\mathbb{T}^n_s \setminus \mathbb{T}^n_{s-1}$. As $M_{s-1}(y') = M_{s-1}(y)$, $R = \operatorname{rank} M_{s-1}(y') \leq \operatorname{rank} M_s(y') \leq R$, where the latter inequality follows from the fact that $y$ is generic, implying $\operatorname{rank} M_s(y') = R$. Hence $\mathcal{B}$ also indexes a maximal linearly independent set of columns of $M_s(y')$. Pick $x^\gamma \in \mathbb{T}^n_s \setminus \mathbb{T}^n_{s-1}$. Then $\operatorname{vec}(x^\gamma - q) \in \operatorname{Ker} M_s(y)$ and $\operatorname{vec}(x^\gamma - q') \in \operatorname{Ker} M_s(y')$ for some $q, q' \in \operatorname{Span}_{\mathbb{R}}(\mathcal{B})$. For any $x^\alpha \in \mathbb{T}^n_{s-1}$, we have $(M_s(y) \operatorname{vec}(q - q'))_\alpha = (M_s(y) \operatorname{vec}(q))_\alpha - (M_s(y') \operatorname{vec}(q'))_\alpha = (M_s(y) \operatorname{vec}(x^\gamma))_\alpha - (M_s(y') \operatorname{vec}(x^\gamma))_\alpha = y_{\alpha+\gamma} - y'_{\alpha+\gamma} = 0$ as $\pi_{2s-1}(y) = \pi_{2s-1}(y')$. Therefore $M_{s-1}(y) \operatorname{vec}(q - q') = 0$, implying $q = q'$ as $q - q' \in \operatorname{Span}_{\mathbb{R}}(\mathcal{B})$ and $\mathcal{B}$ indexes linearly independent columns of $M_{s-1}(y)$. This now implies $M_s(y) \operatorname{vec}(x^\gamma) = M_s(y) \operatorname{vec}(q) = M_s(y') \operatorname{vec}(q') = M_s(y') \operatorname{vec}(x^\gamma)$, i.e. $\pi_{2s}(y) = \pi_{2s}(y')$, giving $\pi_{2s}(z) = 0$. Thus we have shown $\dim \pi_{2s}(\mathcal{K}_t) = \dim \pi_{2s-1}(\mathcal{K}_t)$.

We now show $\pi_{2s}(\mathcal{K}_t) = \pi_{2s}(\mathcal{K}_{t+1})$; it suffices to show the inclusion $\pi_{2s}(\mathcal{K}_t) \subseteq \pi_{2s}(\mathcal{K}_{t+1})$. Let $z \in \mathcal{K}_t$ be generic; we show that $\pi_{2s}(z) \in \pi_{2s}(\mathcal{K}_{t+1})$. Note that $\operatorname{rank} M_s(z) = \operatorname{rank} M_{s-1}(z)$ since both $z$ and $y$ are generic. By Theorem 2.6 there exists an extension $z^* \in \mathbb{R}^{\mathbb{N}^n}$ of $\pi_{2s}(z)$ satisfying $\operatorname{rank} M(z^*) = \operatorname{rank} M_s(z)$ and $\operatorname{Ker} M(z^*) = \langle \operatorname{Ker} M_s(z) \rangle$. From $s \geq D$, it follows that $h_j \in \operatorname{Ker} M_s(z) \subseteq \operatorname{Ker} M(z^*)$, which implies $L_{z^*}(h_j x^\alpha) = 0$ for all $\alpha$, i.e. $z^* \in \mathcal{K}_\infty$. Hence $\pi_{2s}(z) = \pi_{2s}(z^*)$ with $\pi_{2s}(z^*) \in \pi_{2s}(\mathcal{K}_{t+1})$. With $G_t$ denoting the set of generic elements of $\mathcal{K}_t$, we have just shown that $\pi_{2s}(G_t) \subseteq \pi_{2s}(\mathcal{K}_{t+1})$. This implies that $\pi_{2s}(\mathcal{K}_t) \subseteq \pi_{2s}(\mathcal{K}_{t+1})$ since $G_t$ is dense in $\mathcal{K}_t$ (by Corollary 3.1), which concludes the proof. □

REMARK 4.1. The above result combined with the result of Proposition 3.1, which shows that (3.5) holds for *all* $y \in \mathcal{K}_t$ and some $(t, s)$ provides an alternative proof for the termination of the method proposed in [18].

We now prove some converse relation: If (4.3$a$) holds then (3.5) and (3.6) eventually hold too.

PROPOSITION 4.2. *Assume* $\dim \pi_s(\mathcal{K}_t) = \dim \pi_{s-1}(\mathcal{K}_t)$ *with* $D \le s \le \lfloor t/2 \rfloor$, *i.e. (4.3a) holds.*
**(i)** *For all* $y \in \mathcal{K}_{t'}$ *with* $t' := t+s+2d-2$, $\operatorname{rank} M_{s-1+d}(y) = \operatorname{rank} M_{s-1}(y)$.
**(ii)** *For all* $y \in \mathcal{K}_{t''}$ *with* $t'' := t+s$, $\operatorname{rank} M_s(y) = \operatorname{rank} M_{s-1}(y)$.

*Proof.* (i) Recall from the proof of Theorem 4.1 that any $m \in \mathbb{T}^n_s$ can be written as $m = r_m + f_m$, $r_m \in \operatorname{Span}_{\mathbb{R}}(\mathcal{B})$, $f_m \in \operatorname{Span}_{\mathbb{R}}(\mathcal{H}_t)$, $\mathcal{B} \subseteq \mathbb{T}^n_{s-1}$. (Indeed these facts could be proved without using (4.3$b$).) An easy induction on $k \ge 0$ permits to show that any $m \in \mathbb{T}^n_{s+k}$ can be written as $m = r_m + f_m$ where $r_m \in \operatorname{Span}_{\mathbb{R}}(\mathcal{B})$ and $f_m \in \operatorname{Span}_{\mathbb{R}}(\mathcal{H}_{t+k})$. Let $y \in \mathcal{K}_{t'}$. We show that $M_{s+d-1}(y)$ is a flat extension of $M_{s-1}(y)$. For this pick $m, m' \in \mathbb{T}^n_{s+d-1}$. Write $m = r_m + f_m$ with $f_m \in \operatorname{Span}_{\mathbb{R}}(\mathcal{H}_{t+d-1})$ and $r_m = \sum_{b\in\mathcal{B}} \lambda_b b$ ($\lambda_b \in \mathbb{R}$). Then the $(m', m)$th entry of $M_{s+d-1}(y)$ is equal to $L_y(mm') = L_y(m' f_m) + \sum_{b\in\mathcal{B}} \lambda_b L_y(m'b)$. Now $L_y(m' f_m) = 0$ since $m' f_m \in \mathcal{H}_{t'=t+s+2d-2}$ as $f_m \in \mathcal{H}_{t+d-1}$ and $\deg(m') \le s+d-1$. Therefore $(M_{s+d-1}(y))_{m',m} = \sum_{b\in\mathcal{B}} \lambda_b (M_{s+d-1}(y))_{m',b}$, showing that the $m$th column of $M_{s+d-1}(y)$ can be written as a linear combination of its columns indexed by $\mathcal{B}$, i.e. $\operatorname{rank} M_{s-1+d}(y) = \operatorname{rank} M_{s-1}(y)$. The proof for (ii) is analogous. □

PROPOSITION 4.3. *Assume the assumptions of Theorem 4.1 hold. Then for any* $z \in \mathcal{K}_t$, *there exists* $y \in K_\infty$ *with* $\pi_{s-1}(y) = \pi_{s-1}(z)$ *and* $\operatorname{rank} M(y) = \operatorname{rank} M_{s-1}(y)$.

*Proof.* Let $z \in \mathcal{K}_t$. By Theorem 4.1, $\pi_s(z) \in \pi_s(\mathcal{K}_t) = \pi_s(\mathcal{D}[I]) \sim \pi_s(\mathcal{K}_\infty)$. Hence there exists $y \in \mathcal{K}_\infty$ with $\pi_s(z) = \pi_s(y)$. Let $\mathcal{B} \subseteq \mathbb{T}^n_{s-1}$ be a basis of $\mathbb{R}[x]/I$ (use Theorem 4.1). As $I \subseteq \operatorname{Ker} M(y)$, it follows that $\operatorname{rank} M(y) = \operatorname{rank} M_{s-1}(y)$. □

EXAMPLE 5. We consider again Example 2 with $I = \langle x_1^2, x_2^2, x_1x_2\rangle \subseteq \mathbb{R}[x_1, x_2]$, introduced earlier as an example with a non-Gorenstein quotient algebra $\mathbb{R}[x]/I$. The dimension of the space $\pi_s(\mathcal{K}_t)$ for different $t$ and $s$ is shown in Table 4 and the ranks of $M_s(y)$ for generic $y \in \mathcal{K}_t$ in Table 5.

TABLE 4
*Dimension of the set* $\pi_s(\mathcal{K}_t)$ *in Example 5.*

| | $t=0$ | $t=1$ | $t=2$ | $t=3$ |
|---|---|---|---|---|
| $s=0$ | 1 | 1 | 1 | 1 |
| $s=1$ | | 3 | **3** | 3 |
| $s=2$ | | | **3** | **3** |
| $s=3$ | | | | 3 |

Observe that

$$\dim \pi_2(\mathcal{K}_2) = \dim \pi_1(\mathcal{K}_2) = \dim \pi_2(\mathcal{K}_3)$$

TABLE 5
*Rank of $M_s(y)$ for generic $y \in \mathcal{K}_t$ in Example 5.*

| | $t=0$ | $t=2$ | $t=4$ | $t=6$ |
|---|---|---|---|---|
| $s=0$ | 1 | 1 | 1 | 1 |
| $s=1$ | | 2 | **2** | 2 |
| $s=2$ | | | **2** | 2 |
| $s=3$ | | | | 2 |

and

$$\operatorname{rank} M_2(y) = \operatorname{rank} M_1(y) \quad \forall\, y \in \mathcal{K}_4$$

as predicted by Proposition 4.2 (ii).

**5. Conclusion.** In this paper we have presented a new method for computing the complex variety of a zero-dimensional ideal $I$ given by its generators. The method is a complex analogue of the moment-matrix algorithm proposed in [10] for the task of computing the *real* variety of an ideal and its real radical ideal. In contrast to the latter algorithm, the newly proposed method does not use semidefinite optimization and is based purely on numerical linear algebra.

The two methods allow a unified treatment of the algebraic and real-algebraic root finding problems. Remarkably, all information needed to compute the roots is contained in the moment matrix of a single generic linear form associated to the problem. The moment matrix can be computed numerically and, simply by adding or neglecting a positive semidefiniteness constraint, one can move from one problem to the other. While the methods are almost identical in the real and complex cases, substantially different proofs were needed for the complex case.

Furthermore, we have shown how this algorithm is related to other methods in the field, particularly to border basis methods and the Zhi-Reid algorithm based on involutive bases. Indeed, simple relationships between their stopping criteria and the rank conditions used in the moment-matrix method have been established.

In a follow-up paper [9] we show how these other numerical-algebraic methods for complex roots can be adapted to design real-algebraic variants for computing real roots directly by incorporating sums of squares conditions extracted from moment matrices.

## REFERENCES

[1] S. BASU, R. POLLACK, AND M.-F. ROY, *Algorithms in real algebraic geometry*, Vol. **10** of Algorithms and Computations in Mathematics, Springer-Verlag, 2003.

[2] J. BOCHNAK, M. COSTE, AND M.-F. ROY, *Real Algebraic Geometry*, Springer, 1998.

[3] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer, 2005.
[4] ———, *Using Algebraic Geometry*, Springer, 1998.
[5] R. Curto and L. Fialkow, *Solution of the truncated complex moment problem for flat data*, Memoirs of the American Mathematical Society, **119** (1996), pp. 1–62.
[6] A. Dickenstein and I.Z. Emiris, eds., *Solving Polynomial Equations: Foundations, Algorithms, and Applications*, Vol. **14** of Algorithms and Computation in Mathematics, Springer, 2005.
[7] I. Janovitz-Freireich, L. Rónyai, and Ágnes Szántó, *Approximate radical of ideals with clusters of roots*, in ISSAC '06: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation, New York, NY, USA, 2006, ACM Press, pp. 146–153.
[8] A. Kehrein and M. Kreuzer, *Characterizations of border bases*, J. of Pure and Applied Algebra, **196** (2005), pp. 251–270.
[9] J. Lasserre, M. Laurent, and P. Rostalski, *Computing the real variety of an ideal: A real algebraic and symbolic-numeric algorithm.* (Research report, LAAS Toulouse, France, 2007.) Short version in Proceedings of the Conference SAC08, Fortaleza, Brasil, March 16–20, 2008.
[10] ———, *Semidefinite characterization and computation of zero-dimensional real radical ideals.* To appear in Found. Comp. Math., Published online October 2007.
[11] M. Laurent, *Sums of squares, moment matrices and optimization over polynomials.* This IMA volume, Emerging Applications of Algebraic Geometry, M. Putinar and S. Sullivant, eds.
[12] ———, *Revisiting two theorems of Curto and Fialkow*, Proc. Amer. Math. Soc., **133** (2005), pp. 2965–2976.
[13] H. Möller, *An inverse problem for cubature formulae*, Computat. Technol., **9** (2004), pp. 13–20.
[14] B. Mourrain, *A new criterion for normal form algorithms*, in AAECC, 1999, pp. 430–443.
[15] ———, *Symbolic-Numeric Computation*, Trends in Mathematics, Birkhäuser, 2007, ch. Pythagore's Dilemma, Symbolic-Numeric Computation, and the Border Basis Method, pp. 223–243.
[16] B. Mourrain, F. Rouillier, and M.-F. Roy, *Bernstein's basis and real root isolation*, in Combinatorial and Computational Geometry, Mathematical Sciences Research Institute Publications, Cambridge University Press, 2005, pp. 459–478.
[17] B. Mourrain, *Generalized normal forms and polynomials system solving*, ISSAC, 2005: 253–260.
[18] G. Reid and L. Zhi, *Solving nonlinear polynomial system via symbolic-numeric elimination method*, in Proceedings of the International Conference on Polynomial System Solving, J. Faugère and F. Rouillier, eds., 2004, pp. 50–53.
[19] F. Rouillier, *Solving zero-dimensional systems through the rational univariate representation*, Journal of Applicable Algebra in Engineering, Communication and Computing, **9** (1999), pp. 433–461.
[20] F. Rouillier and P. Zimmermann, *Efficient isolation of polynomial real roots*, Journal of Computational and Applied Mathematics, **162** (2003), pp. 33–50.
[21] W. Seiler, *Involution - The Formal Theory of Differential Equations and its Applications in Computer Algebra and Numerical Analysis*, habilitation thesis, Computer Science, University of Mannheim, 2001.
[22] A. Sommese and C. Wampler, *The Numerical Solution of Systems of Polynomials Arising in Engineering and Science*, World Scientific Press, Singapore, 2005.

[23] H.J. Stetter, *Numerical Polynomial Algebra*, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2004.

[24] J. Verschelde, *PHCPACK: A general-purpose solver for polynomial systems by homotopy continuation,* ACM Transactions on Mathematical Software, **25** (1999), pp. 251–276.

[25] A. Zharkov and Y. Blinkov, *Involutive bases of zero-dimensional ideals*, Preprint E5-94-318, Joint Institute for Nuclear Research, Dubna, 1994.

[26] ———, *Involutive approach to investigating polynomial systems*, in Proceedings of SC 93, International IMACS Symposium on Symbolic Computation: New Trends and Developments, Lille, June 14–17, 1993, Math. Comp. Simul., Vol. **42**, 1996, pp. 323–332.